



Data Protection

2025/2026

12th Edition



Contributing Editors:

Tim Hickman & Dr. Detlev Gabel
White & Case LLP

glg Global Legal Group

ISBN 978-1-83918-432-1
ISSN 2054-3786

Published by
glg Global Legal Group
59 Tanner Street
London SE1 3PL
United Kingdom
+44 207 367 0720
customer.service@glgroup.co.uk
www.iclg.com

Publisher
James Strode

Production Editor
Maya Tyrrell

Head of Production
Suzie Levy

Creative Lead
Wilfried Tshikana-Ekutshu

CEO
Jason Byles

Printed by
Ashford Colour Ltd.

Cover image
iStock

Strategic Partners



iclg International
Comparative
Legal Guides

Data Protection 2025

12th Edition

Contributing Editors:

Tim Hickman & Dr. Detlev Gabel
White & Case LLP

©2025 Global Legal Group Limited.

All rights reserved. Unauthorised reproduction by any means,
digital or analogue, in whole or in part, is strictly forbidden.

Disclaimer

This publication is for general information purposes only. It does not purport to provide comprehensive full legal or other advice. Global Legal Group Ltd. and the contributors accept no responsibility for losses that may arise from reliance upon information contained in this publication.

This publication is intended to give an indication of legal issues upon which you may need advice. Full legal advice should be taken from a qualified professional when dealing with specific situations.

Expert Analysis Chapters

- 1** The Rapid Evolution of Data Protection Laws
Tim Hickman & Dr. Detlev Gabel, White & Case LLP
- 8** AI Regulatory Landscape and Development Trends in China
Kate Yin, Gil Zhang, Sherman Deng & Huihui Li, Fangda Partners
- 17** The Increased Relevance for Companies of Data Collection of Racial and Ethnic Origins in the EU
Pierre Affagard & Laure Ekani, Clyde & Co LLP
- 24** Cloud Computing, Privacy Impact Assessments and Record-Keeping Regarding Data Protection in Japan
Yusaku Akasaki, Hiroki Minekawa & Ronald Kaloostian, Chuo Sogo LPC

Q&A Chapters

- 29** **Australia**
Darren Pham, Phillip Salakas & Harry Sultan,
Nyman Gibson Miralis
- 47** **Brazil**
Larissa Galimberti, Luiza Fonseca de Araujo &
Cecília Alberton Coutinho Silva,
Pinheiro Neto Advogados
- 64** **China**
Susan Ning & Han Wu, King & Wood Mallesons
- 81** **Egypt**
Ibrahim Shehata, Tasneem ElNaggar & Safa Rabea,
Shehata & Partners
- 96** **France**
Clara Hainsdorf & Bertrand Liard,
White & Case LLP
- 107** **Germany**
Martin Röleke & Dr. Evelyne Sørensen,
activeMind.legal Rechtsanwalts-gesellschaft mbH
- 120** **Greece**
Dr. Nikos Th. Nikolinakos, Dina Th. Kouvelou &
Alexis N. Spyropoulos, Nikolinakos & Partners Law Firm
- 135** **Hungary**
Adam Liber & Tamás Bereczki,
BLB Legal – Bagdi-Liber-Bereczki Attorneys-at-Law
- 145** **India**
Rachit Bahl, Rohan Bagai, Sumit Ghoshal &
Archana Iyer, AZB & Partners
- 156** **Indonesia**
Abadi Abi Tisnadisastra, Prayoga Mokoginta &
Aloysius Andrew Jonathan,
ATD Law in association with Mori Hamada
- 167** **Ireland**
Victor Timon, Zelda Deasy, Seán O'Donnell &
Jane O'Grady, Byrne Wallace Shields LLP
- 181** **Isle of Man**
Caitlin Gelder, Kathryn Sharman & Sinead O'Connor,
DQ Advocates Limited
- 192** **Israel**
Vered Zlaikha, Ariella May & Shahar Talmon,
Lipa Meir & Co.
- 205** **Japan**
Hiromi Hayashi & Masaki Yukawa,
Mori Hamada & Matsumoto
- 219** **Mexico**
Abraham Diaz, Gustavo Alcocer & Carla Huitron,
OLIVARES
- 229** **Nigeria**
Jumoke Lambo, Chisom Okolie, Opeyemi Adeshina &
Joel Adeyemi Adefidipe, Udo Udoma & Belo-Osagie
- 245** **Pakistan**
Saifullah Khan & Saeed Hasan Khan,
S. U. Khan Associates Corporate & Legal Consultants
- 254** **Poland**
Jakub Gładkowski, Barbara Kieltyka &
Malgorzata Kieltyka, Kieltyka Gladkowski KG Legal
- 271** **Saudi Arabia**
Saifullah Khan & Saeed Hasan Khan,
Droua Al-Amal Consultants
- 282** **Serbia**
Vladimir Djerić, Lena Petrovic, Katarina Radovic &
Kristina Petronijevic, Mikijelj Jankovic & Bogdanovic
- 295** **Singapore**
Lim Chong Kin & Anastasia Su-Anne Chen,
Drew & Napier LLC
- 312** **Switzerland**
Daniela Fábíán, FABIAN PRIVACY LEGAL GmbH
- 322** **Taiwan**
Yvonne Y.F. Lin, Jeffrey K.S. Hung & Jackie Yang,
Formosan Brothers Attorneys-at-Law
- 331** **Ukraine**
Vladyslav Podolyak & Tetiana Partsei, Arriba
- 345** **United Arab Emirates**
Saifullah Khan & Saeed Hasan Khan,
Bizilance Legal Consultants
- 357** **United Kingdom**
Tim Hickman & Aishwarya Jha, White & Case LLP
- 370** **USA**
F. Paul Pittman, Abdul Hafiz & Andrew Hamm,
White & Case LLP

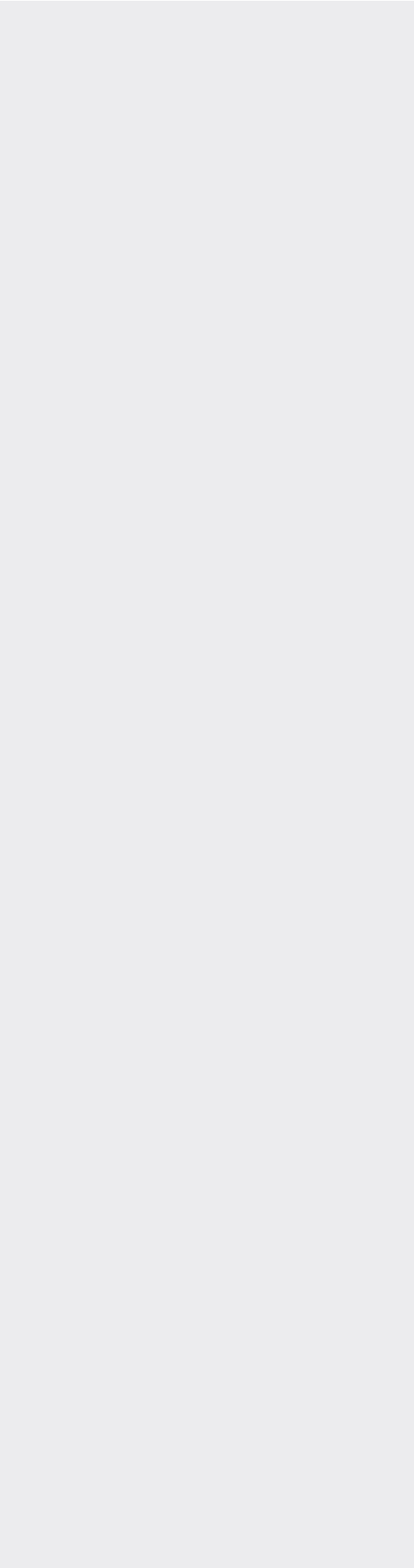
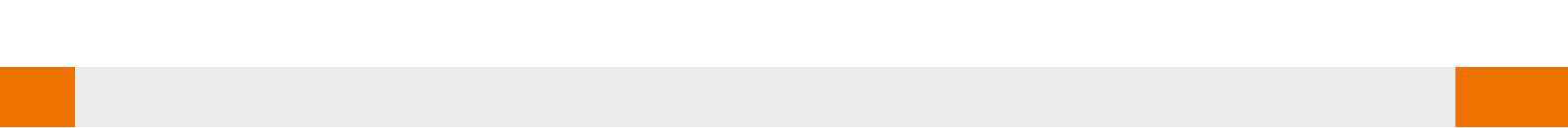
Preface

It is a pleasure to have been asked to provide the preface to *International Comparative Legal Guide – Data Protection 2025*. This edition contains an introductory chapter from White & Case LLP, which briefly charts the technological changes that have driven the evolution of data protection laws in recent decades, and reviews the major challenges that businesses face in complying with the EU's General Data Protection Regulation in particular. It also explores some of the most significant developing trends in privacy laws globally, and illuminates some of the key policy choices that governments will need to consider as they seek to strike a balance between the right to privacy and the development of data-driven economies.

The guide provides 27 question and answer chapters, focusing on key privacy and data protection compliance issues under local laws in countries around the world. This year, new chapters have been added for Egypt, Hungary, Poland and Serbia, which reflects the growth of privacy compliance requirements and challenges in an increasing number of jurisdictions worldwide. As with other entries in the *ICLG* series, this edition provides a go-to resource for anyone seeking practical guidance on these complex legal issues around the world.

Tim Hickman

Partner
White & Case LLP



icl^g

The Rapid Evolution of Data Protection Laws



Tim Hickman



Dr. Detlev Gabel

White & Case LLP

Introduction

Privacy and data protection laws are continuing to adapt to fit an ever-changing world. The evolution of these laws has been especially remarkable over the last two decades. The highly networked and interconnected world in which we live today was merely a glimmer on the horizon in the mid-1990s. The internet itself was still a fairly new innovation to many people. Many businesses did not yet have public websites. Concepts such as online social media platforms did not exist – and certainly nobody had considered how they should be regulated. Virtual reality, smart devices and artificial intelligence (“AI”) have made vast leaps in recent years – all driven by new ways of collecting and using data. Consequently, lawmakers, courts and regulatory authorities have increasingly had to adapt ageing data protection laws to stay abreast of these changes. Privacy and data protection laws are entering a phase of needing near-constant additional guidance, clarification or revision, in order to keep pace with technology.

Developments in the EU – the GDPR and Beyond

Policymakers are being forced to design privacy and data protection laws that are flexible, in order to allow for unforeseen advancements in technology. It is in this context that the EU introduced Regulation (EU) 2016/679 (the General Data Protection Regulation, or “GDPR”) which marked the biggest single shift in data protection laws in Europe since Directive 95/46/EC (the “Directive”) was finalised in 1995.

The GDPR, which has been in effect since May 2018, introduced a range of clarifications and updates, designed to carry EU data protection law forward well into the next decade. It is difficult to overstate the importance of the GDPR. First, it is extremely wide-ranging. The GDPR retains the Directive’s expansive definition of “personal data”, which continues to include all information that relates to any living individual who is identified or identifiable from that information, whether in isolation or in combination with any other available information. This means that almost every business engages in the processing of personal data (e.g., every time an email is sent or received). For many businesses, the GDPR impacts almost every area of operation, from marketing to IT, and from human resources to procurement. Anywhere that information about people is handled, the GDPR follows close behind.

In addition to having a wide subject-matter scope, the GDPR also has an extremely broad territorial scope. It explicitly applies to businesses that are established in the EU, as well as businesses that are located outside the EU that: (i) offer goods

or services to individuals in the EU; (ii) monitor the behaviour of individuals in the EU; or (iii) are established in a place where EU law applies by virtue of public international law (e.g., various overseas territories of EU Member States will fall within this scope).

Mere accessibility of products or services within the EU does not constitute “offering” for these purposes. However, if a business customises any of its products or services for individuals in an EU Member State (e.g., by providing a webpage in a local EU language that would not otherwise be used; by using a local EU top-level domain, such as .eu, .fr or .de; by allowing payment in local currencies such as euros; and/or by mentioning individuals in the EU), then it is likely that EU regulators would consider that the product or service is being “offered” to individuals in the EU, triggering the application of the GDPR. Likewise, “monitoring”, for these purposes, relates to the behaviour of individuals insofar as their behaviour takes place within the EU (e.g., location tracking of individuals; or tracking individuals on the internet, including subsequent profiling, particularly to take decisions concerning such an individual for analysing or predicting that individual’s personal preferences, behaviours and attitudes, would amount to monitoring). In summary, if a business (even one based outside the EU) wants to interact with individuals within the EU, then it needs to do so in compliance with the GDPR.

Second, the GDPR carries serious penalties. EU legislators and regulators have expressed the view that, for too long, businesses have not taken their data protection compliance responsibilities seriously enough. The challenge has been that the cost of compliance with EU data protection law is undeniably high. Implementing all of the right processes, procedures, policies and agreements requires time, effort and expertise, none of which come cheaply. Conversely, the risk of enforcement has historically been relatively low. EU regulators generally have limited resources that are significantly stretched, and enforcement in respect of every breach is simply not feasible. The introduction of the GDPR has stretched these resources further, as regulators have had to deal with a wave of new data breach reports from businesses. They have also faced greater competition for competent data protection practitioners from private companies that are increasingly eager to hire experienced advisors. In addition, in the event that penalties are issued in respect of a breach of EU data protection law, the level of such penalties was comparatively low under the Directive. When considered in the light of penalties for breaches of competition law or financial regulatory law, EU data protection penalties have, in the past, seemed trifling by comparison. The GDPR provided an opportunity to redress this balance. While there was little prospect of reducing the

cost of compliance or increasing the frequency with which penalties could be applied, there was clearly scope to ensure that the severity of the penalties could be increased. After much negotiation, the EU settled on a dramatic increase of the maximum penalties for non-compliance under the GDPR, to the greater of EUR 20 million, or 4% of worldwide annual turnover – numbers that are specifically designed to attract C-Suite attention.

Third, the GDPR requires substantial openness and transparency – the level of detail that businesses are required to disclose in policies and notices regarding their processing activities is extensive. The GDPR imposes tight limits on the use of personal data, especially in the context of direct marketing and certain types of profiling, against which individuals are granted an automatic right to object.

Lastly, the GDPR grants individuals powerful rights that can be enforced against businesses (e.g., the right of individuals to gain access to their personal data, and to be informed about how those data are being used; the “right to be forgotten”, which permits individuals to require businesses to erase their personal data in certain circumstances; and the right to data portability).

Satisfying these requirements has proven to be a serious challenge for many businesses. Indeed, even if a business has all of the right systems, procedures, policies and agreements in place, and has provided all appropriate training to its employees, it cannot guarantee that its employees will never depart from that training and place the business in breach of the GDPR. In addition, no matter how good a business’s cybersecurity measures are, it can never guarantee that no third parties will be able to gain unauthorised access to personal data on its systems. As a result, businesses are well advised to think of GDPR compliance as an exercise in continually identifying and addressing compliance risks. For as long as new technologies continue to provide us with new ways to use data, this process of spotting data protection risks and working out how to solve them will remain necessary. It should also be noted that each EU Member State has passed its own GDPR implementation measures, meaning that there continue to be some national variations from one EU Member State to the next.

While businesses are increasingly reliant on courts and regulators to clarify the application of these rules in light of new technological developments, the GDPR remains a significant cornerstone of the EU’s digital policy. On 25 July 2024, the European Commission published its second report on the application of the GDPR, highlighting areas in which the GDPR had been effective, and areas in need of improvement. The report stresses the need for consistent interpretation and enforcement of the GDPR across the EU, highlighting “ongoing challenges such as divergent national interpretations, difficulties in cooperation among regulatory bodies, and obstacles faced by organisations in achieving compliance”.

Beyond the GDPR, the EU continues to issue new laws that impact privacy and data protection. The first of those laws is the Directive on security of network and information systems (the “**NIS Directive**”), which imposes minimum cybersecurity standards on operators of essential services (i.e., services that are structurally or economically important) and digital service providers (which includes all providers of online services and platforms). Businesses falling within these categories are required to take steps to ensure that their cybersecurity arrangements meet certain minimum thresholds. In the event of a data breach, these businesses will also be subject to mandatory data breach reporting obligations. To address the challenges stemming from the increasing

digital transformation (intensified by the COVID-19 crisis), the European Commission adopted a proposal for a revised Directive on security of network and information systems (the “**NIS2 Directive**”), which entered into force on 16 January 2023. The aim of the NIS2 Directive is to uplift the overall level of cybersecurity across a wide range of organisations operating in the EU. In particular, key elements of the NIS2 Directive include an expansion of the scope of the NIS Directive by adding new sectors based on their criticality for the economy and society, and the strengthening of cybersecurity obligations for affected businesses, including obligations focused on the requirement to effectively address cybersecurity risks in supply chains and supplier relationships, organisational governance and operational risk-management and cyber-incident reporting, and the introduction of more stringent supervisory measures for national authorities. Each EU Member State was required to have implemented laws in their own jurisdiction to give effect to the NIS2 Directive by 17 October 2024. The European Commission opened infringement procedures against 23 Member States after they failed to comply with this deadline.

Some EU Member States (such as Belgium and Italy) have since implemented the NIS2 Directive into national legislation, while others (including Germany and France) remain in the drafting phase. Meanwhile, in March 2024, the European Parliament approved an additional set of rules to protect consumers and businesses from products with inadequate security features (the “**Cyber Resilience Act**”). A first ever EU-wide legislation of its kind, the Cyber Resilience Act, aims to introduce mandatory cybersecurity requirements for products with digital elements and obligations on all economic operators involved throughout their lifecycle. It also establishes a market surveillance and enforcement system, requiring Member States to designate authorities to monitor compliance and impose measures for non-compliance (e.g., fines of up to EUR 15 million or 2.5% of total worldwide annual turnover in the previous financial year for non-compliance with essential cybersecurity requirements). The Cyber Resilience Act entered into force on 10 December 2024. Companies operating across multiple jurisdictions should continue to familiarise themselves with the cybersecurity laws applicable to their operations (e.g., when designing cybersecurity breach response strategies and cybersecurity risk-management frameworks, or engaging “ethical hacker” services), and ensure that they understand the regulatory reporting obligations that are triggered if a cybersecurity breach occurs.

After years of no material developments, the European Commission confirmed in February 2025 that the proposed e-Privacy regulation had been withdrawn. Nevertheless, enforcement-related developments in the EU based on the existing ePrivacy framework continue. On 17 January 2023, the European Data Protection Board (the “**EDPB**”) adopted a report of the work undertaken by the Cookie Banner Taskforce established in September 2021 to investigate and coordinate a response to the growing number of complaints concerning cookies throughout the EEA (the “**Cookies Report**”). The Cookies Report sets out a number of observations regarding the common issues with respect to use of cookie banners. For instance, the Cookies Report identifies the following practices considered non-compliant by EU Data Protection Authorities: (i) including a button that permits individuals to accept the storage of all cookies, but that fails to also include a button that permits individuals to reject the storage of all cookies; (ii) including pre-ticked boxes for consent to one or more categories of non-essential cookie storage (i.e., this practice is

non-compliant with the applicable requirements); and (iii) using practices that EU Data Protection Authorities consider “deceptive” to nudge individuals into accepting storage of non-essential cookies (e.g., use of colour/contrasts to highlight the “accept all cookies” button over other available options). On 16 November 2023, the EDPB also published guidelines to clarify the scope of the EU cookie notice and consent requirements. The guidelines explain the elements that trigger an obligation to obtain opt-in consent under Article 5(3) of the ePrivacy Directive, which includes: (1) information; (2) terminal equipment; (3) electronic communications network; (4) gaining access; and (5) stored information and storage.

One major development has been the issue of “pay or consent” models. On 17 April 2024, the EDPB adopted an Opinion on “Valid Consent in the Context of Consent of Pay Models implemented by Large Online Platforms”. The EDPB considered that, in many cases, it would likely not be possible for large online platforms to comply with requirements under the GDPR if they only provide users with a binary choice, i.e., users can choose to consent to the processing of personal data for behavioural advertising purposes or pay a fee. However, there remains material uncertainty as to how this interpretation will be applied in practice.

Following the decision of the Court of Justice of the European Union (the “CJEU”) in *Schrems II* (Case C-311/18), the European Commission published an Implementing Decision adopting new standard contractual clauses (the “Revised SCCs”) for the transfer of personal data outside the EEA. The Revised SCCs address various known shortcomings of the standard contractual clauses originally published in 2001 and 2010, many of which were noted by the CJEU in *Schrems II*, as well as imposing new requirements (for instance, requiring that the laws and practices in the data importer’s jurisdiction should be assessed by the data exporter for compatibility with the GDPR, prior to exporting personal data). The Revised SCCs, which came into force on 27 June 2021, adopt a modular approach, taking into account various transfer scenarios depending on the relationships between the parties (i.e., Controller to Controller, Controller to Processor, Processor to Processor, and Processor to Controller). Since 27 December 2022, only the Revised SCCs can be used. Any agreements that use one of the older versions of the standard contractual clauses (i.e., the 2001, 2004 or 2010 versions) are now invalid, and need to be replaced with the Revised SCCs. The European Commission announced in September 2024 that it was consulting on a new set of SCCs that were intended to address data transfers to third countries, where the recipient is already subject to the GDPR. These SCCs are expected to be a simplified version of the Revised SCCs and are expected to be implemented in the second half of 2025.

In the realm of cross-border data transfers, the European Commission and the US White House announced in March 2022 that they had reached an agreement in principle on a new “Trans-Atlantic Data Privacy Framework” (the “EU-US Data Privacy Framework”) to succeed the EU-US Privacy Shield, which was effectively invalidated by the CJEU in *Schrems II*. The announcement came against the backdrop of extensive negotiations between the EU and the US following *Schrems II*. The EU-US Data Privacy Framework is described as reflecting the “unprecedented commitment” of the US to reform its privacy and civil liberties protections that apply to its signals intelligence/surveillance activities. Notably, the EU-US Data Privacy Framework seeks to establish a “Data Protection Review Court” as part of its new two-tier redress system to resolve EU residents’ complaints against unlawful

access of their personal data by US intelligence authorities. Following the announcement, on 7 October 2022, then-President Biden signed an executive order to implement the agreement made in March 2022 into US law. The European Commission adopted its adequacy decision on 10 July 2023, enabling transfers of personal data from the EEA to the certified US recipients to be made without use of the Revised SCCs, binding corporate rules, etc. In October 2024, the European Commission published its findings on the adequacy decision from 10 July 2023, holding that US law provides an adequate level of protection for personal data transferred from the EU to the US if the recipient organisation is certified under the EU-US Data Privacy Framework.

Finally, as part of its “European Strategy for data”, the European Commission has imposed new sets of rules on the neutrality of data marketplaces (the “Data Governance Act”) and has proposed new rules on the use of, and access to, data generated in the EU across all economic sections (the “Data Act”).

The Data Governance Act creates new rules on the neutrality of data marketplaces by allowing novel “data intermediaries” to function as trustworthy organisers of data sharing, boost trust in data sharing by providing more control to EU citizens and companies over the use of the data they generate, and facilitate the re-use of certain data held by the public sector. The Data Governance Act entered into force on 23 June 2022 and, following a 15-month grace period, has been applicable since September 2023.

Separately, the Data Act aims to ensure fairness in the digital environment, stimulate a competitive data market, open opportunities for data-driven innovation and make data more accessible across the EU. Notably, it proposes to provide legal certainty for consumers and businesses to access data generated by the products or related services they own, rent or lease; and protect SMEs from unfair contractual terms by devising an “unfairness test” against which unilaterally imposed contractual clauses will be measured. The Data Act entered into force on 11 January 2024 and, following a 20-month grace period, will be applicable from September 2025.

On the topic of AI, Regulation (EU) 2024/1689 (the “AI Act”) aims to provide a horizontal legal framework for AI regulation across the EU. The AI Act imposes: (i) a definition of “AI systems”; (ii) a risk-based approach (to determine whether an AI system can be lawfully developed and the risks posed to fundamental rights); (iii) obligations on various actors throughout the AI life cycle; and (iv) penalties for non-compliance of up to the greater of EUR 35 million or 7% of worldwide annual turnover. The AI Act entered into force on 1 August 2024. It has slowly become applicable since 2 February 2025, but the enforcement of the majority of its provisions will commence on 2 August 2026. In June 2024, the EDPS published guidelines regarding generative AI and personal data, that were intended to “... provide some practical advice to the EU institutions, bodies, offices and agencies on the processing of personal data in their use of generative AI systems, to ensure that they comply with their data protection obligations”. Meanwhile, a large number of other jurisdictions are in the process of preparing their own AI regulations, and the impact of these changes on the processing of personal data remains to be seen.

Developments Outside the EU

While the EU may have issued the most far-reaching data protection law to date, it is important to note that a large number of other jurisdictions have introduced, or are in the

process of introducing, laws to tackle the challenges that modern technology presents in a privacy and data protection context. The nature and scale of these laws vary significantly. As a result, businesses continue to face different data protection compliance obligations from one jurisdiction to the next. Some of these changes have been driven by the GDPR. For example, several jurisdictions that currently benefit from adequacy decisions from the European Commission (permitting the transfer of personal data from the EU to those jurisdictions without additional data transfer safeguards) have updated their domestic data protection laws with a degree of congruity with the GDPR. The reason for this is that, under the GDPR, adequacy decisions have a shelf life. As a result, jurisdictions such as Canada and Switzerland have revised their local data protection laws to implement standards that will more closely match the GDPR. On 15 January 2024, the European Commission announced that it has concluded its review of 11 existing adequacy decisions and that personal data transferred from the EU to Andorra, Argentina, Canada, the Faroe Islands, Guernsey, the Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay continues to benefit from adequate data protection safeguards.

Meanwhile, following Brexit, the GDPR has been retained in UK law with a few amendments. The amended GDPR (the “**UK GDPR**”) and the Data Protection Act 2018 now form the principal pieces of data protection legislation in the UK. The UK GDPR is broadly aligned with the GDPR in terms of its substantive requirements. However, provisions concerning supervisory bodies and interactions between EU Member States have been amended to reflect the fact that the UK is no longer directly subject to EU law and enforcement regimes. Powers previously held at the EU level are now held by the UK’s Information Commissioner’s Office (“**ICO**”).

In 2025, the ICO released guidance on the use of personal data as part of a “pay or consent” business model, following a public consultation on draft proposals (discussed above in the context of the EU). The ICO guidance acknowledges the rise of consent or pay models and reaffirms that such models are not intrinsically non-compliant with the UK GDPR. However, the guidance emphasises the importance of obtaining valid consent, in accordance with the requirements of the UK GDPR.

Separately, as a result of Brexit, the UK became a “third country” for the purposes of EU law, which initially led to a brief period of uncertainty regarding transfers of personal data between the EU and the UK. By way of background, the UK was involved in the drafting of both the Directive and the GDPR, and has had significant input into the preparation of regulatory guidance issued by EU regulators in the last two decades. After Brexit, the EU assessed whether the UK should receive an adequacy decision under the GDPR. On 28 June 2021, the European Commission adopted two adequacy decisions (the “**UK Adequacy Decisions**”): one in relation to the GDPR (which considered, among other things, the UK’s general data protection framework and the level of access that the UK Government has to personal data for law enforcement and national security purposes); and one in relation to the Law Enforcement Directive (which assessed the UK’s standards regarding police and judicial cooperation in criminal matters, among other factors). However, the European Commission included a “sunset clause” in the UK Adequacy Decisions, which serves to limit the validity of the decisions to four years. Both of the UK Adequacy Decisions originally were set to last until 27 June 2025, at which stage the continued suitability of the UK Adequacy Decisions was to be reassessed by the European Commission. However, on 18 March 2025,

the European Commission announced plans to extend the UK Adequacy Decisions until 27 December 2025. The European Commission has stressed that this extension is “exceptional”, presumably with a view to give the UK time to conclude the legislative process for the proposed Data (Use and Access) Bill (the “**DUA Bill**”) (noting that the DUA Bill, once finalised, will impact the EU’s assessment on the equivalence of UK data protection law). As an introduction to the DUA Bill, note that it is a draft law designed to implement a number of provisions, including those related to “... access to customer data and business data” and “services consisting of the use of information to ascertain and verify facts about individuals”. The DUA Bill is working its way through parliament, and at the time of writing, is currently in its final stages. Please see further below for more background on the DUA Bill.

On the topic of data transfers, following the EU’s adoption of an adequacy decision in respect of the EU–US Data Privacy Framework, the UK Government has also laid out adequacy regulations to extend the EU–US Data Privacy Framework to data transfers from the UK to the US before Parliament on 21 September 2023 (the “**UK–US Data Bridge**”). Since 12 October 2023, the UK–US Data Bridge has permitted the transfer of personal data to participating US organisations, without the need for transfer mechanisms or transfer risk assessments that would otherwise be required.

In a step towards divergence with the EU approach, on 21 March 2022, the ICO adopted its counterpart to the EU’s Revised SCCs in the form of an international data transfer agreement (the “**IDTA**”) and an international data transfer addendum to the Revised SCCs for international data transfers (the “**UK Addendum**”). All contracts concluded after 21 September 2022 are now required to use either the IDTA or the UK Addendum (as appropriate) for international transfers of personal data to jurisdictions that do not benefit from adequacy regulations under the UK GDPR.

Separately, following a public consultation in early 2022, the UK Government launched an open consultation on its proposal to address the deficiencies in the UK’s cybersecurity laws framework. The UK’s current cybersecurity laws are largely based on the NIS Directive (which the UK had transposed into domestic law pre-Brexit). While the proposed modernisation of the UK’s cybersecurity framework is currently in its infancy, the approach differs substantially from the NIS2 Directive, and can be expected to create significant divergence between the two regimes if formalised along the lines of the UK Government’s current proposal. It is expected that this updated legal framework will cover a broader range of organisations, amend the approach to regulatory oversight, and broaden the scope of cyber-incidents that must be reported to regulators and affected individuals. The UK Government continues to consult on an update to the Computer Misuse Act 1990 – a piece of ageing legislation that criminalises the activities of cybercriminals. Changes to the cybersecurity legislative framework are likely to influence many organisations’ data protection compliance programmes, particularly from data security and breach reporting perspectives.

Many other jurisdictions have implemented, or are in the process of implementing, new comprehensive national data protection compliance requirements.

Across the Atlantic, major developments have occurred in the United States, with an increasing number of state data privacy laws (California, Utah, Colorado, Connecticut, Virginia, Iowa, Indiana, Tennessee, Montana, Florida, Texas, Oregon, Delaware, Nebraska, New Hampshire, New Jersey, Minnesota, Maryland) that are already in effect or will take

effect later in 2025. Further, a comprehensive federal privacy law is also being mooted; although, at the time of writing, this has not been progressed. President Donald Trump passed Executive Order 14117 on “Preventing Access to Americans’ Bulk Sensitive Personal Data and United States Government-Related Countries of Concern”, which aims to prevent access to Americans’ sensitive personal data and United States Government-related data by “countries of concern” and associated entities.

In Asia, the Personal Information Protection Law of the People’s Republic of China came into effect on 1 November 2021, and on 22 March 2024, final regulations were published by the Cybersecurity Administration of China concerning outbound data transfers of personal information and “important data” from China to other jurisdictions. Outbound data transfers include situations in which an entity in China actively sends data to a recipient in another jurisdiction, or permits a person or entity outside China to access data generated in the course of the data processor’s operations in China. Failure to comply with the applicable requirements regarding outbound data transfers may result in administrative, civil and criminal penalties. On 18 September 2024, a new “Guide for Sensitive Personal Information Identification” was published by China’s National Information Security Standardization Technical Committee. These guidelines provide rules related to the use of “sensitive personal information”, and also define “personal information” as information that “... will be regarded as sensitive if its disclosure or illegal use will easily result in damage to the dignity of natural persons, or endanger personal safety or properties”.

Thailand’s Personal Data Protection Act came into effect on 1 June 2022, and in August 2024, the first major enforcement decision under the Act was made against an IT retailer. Sri Lanka’s new Personal Data Protection Act officially came into force in July 2023, and four provisions of the Act have been in effect since January 2024. India’s Digital Personal Data Protection Act came into effect on 11 August 2023 and is now part of the personal data protection and regulatory regime in India.

In the Middle East, the United Arab Emirates’ new federal Data Protection Law came into effect on 2 January 2022, and the new Omani Personal Data Protection Law came into effect on 13 February 2023. The Kingdom of Saudi Arabia’s Personal Data Protection Law came into effect on 23 March 2022, and enforcement has been in effect since September 2024. In August 2024, the Israeli Parliament approved a major amendment to the Israeli Privacy Protection Law 1981, which is expected to enter into force in August 2025.

A smaller but growing trend has been data localisation. This term refers to national laws that require the storage of data locally within the relevant jurisdiction. This is subtly different to data transfer restrictions. Whereas a data transfer restriction law limits the ability of businesses to send data internationally without valid protections in place, a data localisation law is often less concerned with international data transfers, provided that at least one complete copy of the data remains in the relevant jurisdiction. Arguably, the best-known example is Russia, which introduced a major data localisation law in 2015 that applies to all personal data of Russian citizens. A number of other jurisdictions have data localisation requirements that are either limited to particular technologies (e.g., German law requires telecoms companies to store communications metadata locally) or particular sectors (e.g., Australia requires health data to be stored locally). This trend is moving in two different directions simultaneously. In the EU, there is

pressure for all such localisation requirements to be removed, to allow a truly free flow of data within the bloc. However, in a number of other parts of the world, including China, data localisation laws are becoming increasingly popular, and in some cases are being used as a means of digital protectionism. Applicable laws in India, too, favour the latter position.

Future Uncertainty

In March 2023, the UK’s Department for Science, Innovation and Technology (the “**DSIT**”) introduced the Data Protection and Digital Information (No.2) Bill (the “**Data Protection Bill**”) to the UK Parliament for consideration. The Data Protection Bill was claimed to be “an important milestone in the evolution of the UK’s data protection regime” (in the ICO’s words), and was designed to amend the UK’s Data Protection Act 2018, the UK GDPR and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (“**PECR**”). It would have seen the UK data protection legal landscape diverge from the GDPR and the ePrivacy Directive in a number of important areas. However, this Bill did not proceed, due to the 2024 General Election which led to a change in government.

As noted above, the new UK government is progressing the DUA Bill through Parliament. The DUA Bill, which is currently in its final legislative stages, is similar to the Data Protection Bill in some areas. The DUA Bill proposes to: (i) extend the “smart data” model (which allows consumers to request their data be shared directly with authorised and regulated third parties), currently used in open banking, to other sectors such as energy, telecommunications, and insurance; (ii) regulate the provision of digital verification services through the creation of a trust framework, a register of providers, an information sharing gateway, and a trust mark; (iii) put the national underground asset register on a statutory footing; (iv) update the way births and deaths are registered, moving from a paper-based system to an electronic register used by officials; (v) proposes material changes to the UK’s data protection regime regarding the ICO’s enforcement powers under PECR, cookie consent, data subject right requests, automated decision-making, and legitimate interests (among other things); (vi) proposes to abolish the ICO and transfer its functions to a new body, the Information Commission; and (vii) make further provision about the use of, or access to, data in various areas, including online safety and public service delivery.

Policy Considerations

Global privacy laws are, as ever, at a crossroads. To date, these laws have tended to focus heavily on the rights of individuals. The aim has generally been to ensure that individuals’ private lives are protected, and are not unfairly infringed upon by governments and businesses. However, interesting new facets are emerging in discussions about the future direction of policy in this area. On the one hand, there is strong business pressure to allow the free flow of data, as a necessary part of a world in which economic growth is increasingly digital. On the other hand, individuals generally do not like the feeling that they are being spied upon, or that their data are somehow out of their control. The overall approach to this issue in the EU, and certain other jurisdictions, is now settled for the foreseeable future, but lawmakers in jurisdictions where privacy is a growing theme (notably the US) have hard decisions ahead of them.

Many countries wrestle with the question of how to balance the right to privacy and the ability of companies to monetise data about individuals. On the one side, there is the

suggestion that the right to privacy is absolute and inviolable (indeed, in the EU it is referred to as a “fundamental right”). Proponents of this view consider that the right of individual privacy is paramount, and that businesses should be made to work around it – and it is not hard to see why this argument is appealing. Large data breaches and failures of security hit the headlines with alarming regularity and illustrate that many businesses are not investing nearly as much in digital security as they should. Indeed, even where proper and responsible investment has been made, it is often impossible for any business to ensure that no well-funded third-party attacker can get into its systems.

In addition to the problems surrounding breaches of security, businesses are often found to have been less than totally forthcoming with individuals about how their data will be used, and with whom those data will be shared. Those businesses that do provide accurate and complete information on this issue tend to do so in privacy notices that are often challenging for the average person to interpret and apply in the context of their own lives. Consequently, there is sympathy with the idea that governments should set policies that will force businesses to take a much more protective approach to the data they handle.

The counter-argument is that while individuals often indicate in surveys that they are concerned about privacy, their actions and their spending habits reveal something else. When offered the choice between a free service that is funded through personalised advertising based on tracking of the individual user’s behaviour, or a service that is more privacy-friendly but that must be paid for by the user, the free (but privacy-invasive) service has proven overwhelmingly more popular. Individual users have a tendency to express concern regarding their privacy, while continuing to prefer services that are funded through the processing of their personal data. As a result, policymakers outside the EU have tended to stop short of introducing laws that would prohibit outright the provision of services in exchange for the invasive collection of data, on the basis that to do so would rob individuals of access to services they clearly want to use, even where such access comes at the price of invasive use of their data.

A further policy consideration has emerged. New technologies, including machine learning, AI and fintech, offer untold benefits in terms of analysis of data and fast, accurate decision-making in tasks that might take a human significantly longer. However, the training and development of these technologies is often reliant on access to vast pools of data in order to produce meaningful results. Developers are facing hard choices about whether to move their operations to jurisdictions that place fewer restrictions on the handling of data for training purposes. In addition, once products are operational, many businesses are finding that they face a high regulatory hurdle if they decide to offer their services into jurisdictions with very strict privacy laws and new AI regulatory regimes. Some businesses have started to take the view that the cost of satisfying such strict privacy and AI regulatory compliance obligations is too high to justify, until the product is well established. As a result, users located in jurisdictions

with strict privacy laws and AI regulatory regimes are increasingly finding that the latest technologies are not available in their jurisdictions. It is therefore important for all jurisdictions to ensure that they implement privacy laws and AI regulatory regimes in a way that does not inhibit creativity and technological development. If they fail to do so, they risk turning their citizens into second-class passengers on the digital journey.

When Businesses Find Themselves Surrounded by Uncertainty, Where Should They Start?

The key message for businesses is that there is an inexorable move towards a world in which laws and regulations will more tightly restrict the ways in which personal data can be used. Many of these laws and regulations present unknown future risks, and give rise to uncertainty. However, commerce is increasingly dependent upon data – businesses that considered themselves to be manufacturers, transportation companies or supermarkets as recently as five years ago are now finding that their ability to extract value from transactions is ever more reliant upon the availability of accurate data. Caught between a dependence on data, and the risk of laws that restrict the use of data, businesses should be forward-thinking and plan ahead.

Businesses should start by identifying and addressing the biggest compliance risks they face under the GDPR and other applicable laws, and should address those risks in order of severity of impact. It is often possible to generate quick wins by meeting easy-to-complete requirements such as the update or creation of privacy policies, notices, contracts with customers and vendors, and other key documentation.

One of the most significant risks is that nobody will take responsibility for data protection compliance unless they are required to do so. Therefore, it is generally advisable to ensure that responsibility for ongoing compliance is allocated to someone, and that there is a mechanism for checking on progress. As part of this process, businesses should seek to build awareness of data protection and privacy expectations and requirements among their staff members, and ensure that the operational impact is well understood by staff who process personal data.

Last, but by no means least, businesses should see this as an opportunity. Lawmakers are taking privacy and data protection seriously because the public increasingly does so too. A well-planned and well-executed privacy compliance programme can provide a competitive advantage by helping a business to ensure that its customers, suppliers and employees feel confident in allowing that business access to their data – which is increasingly the lifeblood of today’s digital world.

Note

This publication is provided for your convenience and does not constitute legal advice. This publication is protected by copyright.



Tim Hickman is a partner in the London office of White & Case and is head of the Firm's Data, Privacy & Cybersecurity practice. He advises on all aspects of data protection law and AI regulation. Tim has significant experience of working with a wide range of clients in the UK, the EU, Asia and the US.

"Working with Tim Hickman has been a pleasure, I'm continually impressed with his depth of knowledge and experience in handling complicated privacy compliance issues. One of the most significant advantages of working with Tim is his ability to coordinate efficiently with other countries' colleagues at W&C to deliver what we ask in a cost-effective approach." – *The Legal 500, UK 2025*.

White & Case LLP

5 Old Broad Street

London EC2N 1DW

United Kingdom

Tel: +44 20 7532 2517

Email: tim.hickman@whitecase.com

LinkedIn: www.linkedin.com/in/tim-hickman



Dr. Detlev Gabel is a partner in the Frankfurt office of White & Case and a member of the Firm's Global Cyber Risk Committee.

Detlev advises multinational clients on a broad range of data protection and cybersecurity matters, including European and German data protection law compliance, cross-border data transfers and data breach response issues.

Detlev frequently publishes and speaks on topics relating to the aforementioned areas. Notably, he is the co-editor and co-author of highly regarded treaties on data protection law and cybersecurity law, and lectured for almost 10 years on data protection law at the University of Oldenburg, Germany, in a course leading to a Master's of IT Law.

"Detlev Gabel is a leading data protection specialist who advises on cyber attacks and large outsourcings and also acts for clients in front of data protection authorities." – *Chambers Europe 2024*.

White & Case LLP

Bockenheimer Landstraße 20

60323 Frankfurt am Main

Germany

Tel: +49 6929 9940

Email: dgabel@whitecase.com

LinkedIn: www.linkedin.com/in/detlevgabel

With one of the largest and most experienced data privacy and cybersecurity groups in the world, White & Case's global team is on hand to guide clients through the relevant data protection legislation in the jurisdictions in which they are active. Seamlessly working with their counterparts in other practice areas, our global team has the depth of resources to provide integrated, creative and practical advice on the privacy-related concerns faced by our clients, wherever they are located.

Our experience spans the full range of industry sectors including financial institutions and banking, biotechnology, pharmaceuticals and chemicals, construction and engineering, consumer goods and retail, automotive, hotels and leisure, IT, telecommunications, internet and social media, manufacturing and electronics, publishing and media.

www.whitecase.com

WHITE & CASE

AI Regulatory Landscape and Development Trends in China

Fangda Partners



Kate Yin



Gil Zhang



Sherman Deng



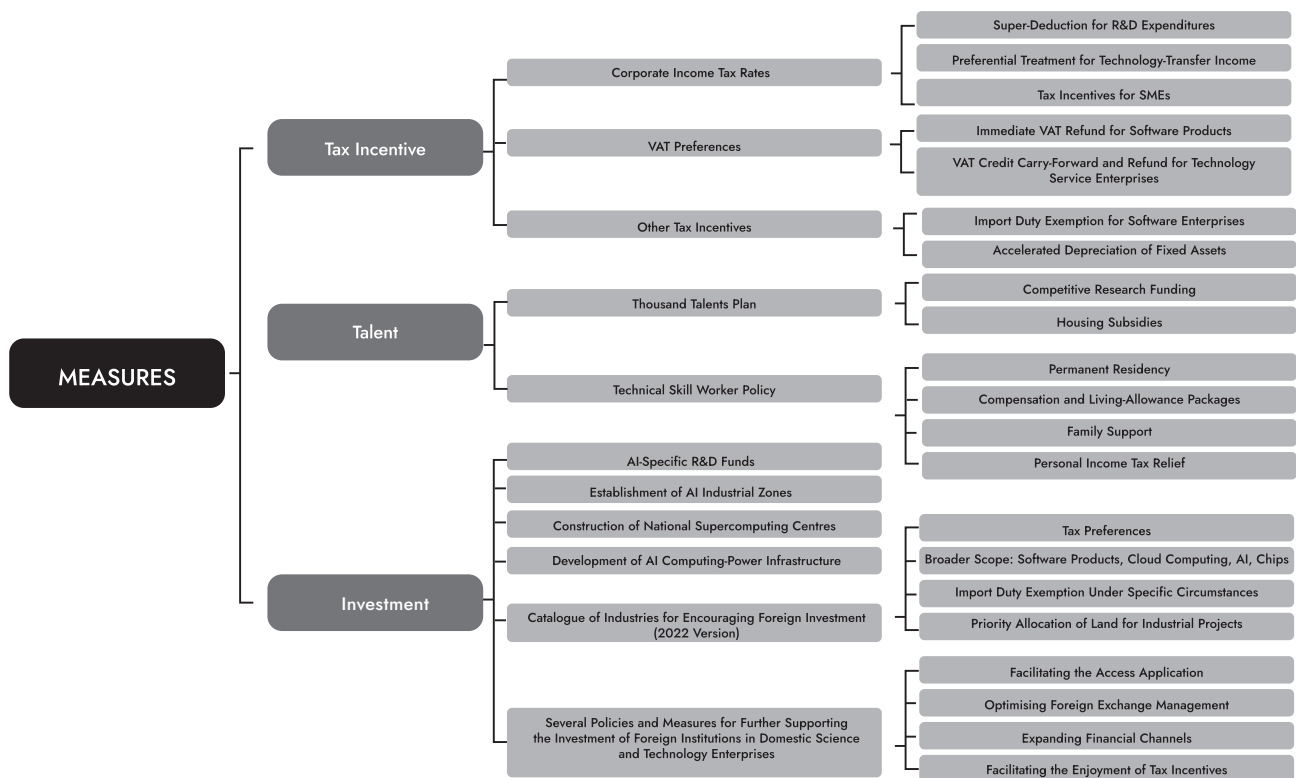
Huihui Li

1. Public Policy and AI Development State of Play

China promotes development of AI and international collaboration

China has made great progress in artificial intelligence (AI) through strategic plans and initiatives since 2016. The Chinese government has rolled out a series of blueprints and public policies, aiming to support AI companies on various fronts such as talent cultivation, startup incubation, computing power and infrastructure procurement, investment schemes, incentives and taxation, product marketisation and other related aspects.¹

Aside from promoting the development of the domestic AI industry, in October 2023, at China's Belt and Road Forum, President Xi Jinping announced a new Global AI Governance Initiative, which calls for developing countries to participate in AI governance and expresses concerns over data abuse and the use of AI in terrorism and other criminal activities. The Initiative also calls for global collaboration to foster the sound development of AI, share AI knowledge, and make AI technologies available to the public under open-source terms, and opposes creating barriers and disrupting the global AI supply chain through technological monopolies and unilateral coercive measures. As commented by the spokesperson from the Chinese Foreign Ministry: "China stands ready to have exchanges and practical cooperation with all sides on global AI governance and deliver benefit for all human beings through AI technology."²



China's sectoral AI adoption is also growing fast – most notably in healthcare – as China's AI ecosystem is thriving under a wave of supportive policies.

- **MedTech:** As encouraged by the Reference Guidelines for AI Application Scenarios in the Health and Wellness Industry as released by the National Health Commission in November 2024, many public hospitals have since started to deploy DeepSeek or HuatuoGPT and thus have delivered remarkable results in diagnostics, medical imaging analysis, intelligent triage and chronic disease management.
- **Online services:** Major shopping platforms, e-commerce sites and short-video apps all deploy AI algorithms for content feeds, payments and user services. The government has likewise pushed “smart retail” upgrades. Retailers are adopting AI for inventory, cashier-free shopping and even generative design of products.
- **Robot and manufacturing automation:** Robotics companies have deployed their AI-driven quadruped inspection robots across manufacturing, warehousing and energy facilities, leveraging real-time computer vision and autonomous navigation for tasks like urban travel, perimeter patrol, equipment inspection and material transport.
- **General-Purpose AI:** Major Chinese tech companies have launched numerous large language models (LLMs). As of March 2025, approximately 350 LLMs have been filed with Chinese regulator Cyberspace Administration of China (CAC), which include companies and applications covering fintech, medical and healthcare, education, intelligent manufacturing, content creation, and enterprise services.

Ethics principles and responsible use of AI

As evidenced in various Chinese regulations and public policies, the Chinese government has adopted a “people-centred” approach in AI-related policy-making and legislative work, embedding principles of safety, fairness, transparency and controllability throughout the AI lifecycle. At the same time, it has produced industry-wide standards and ethical review mechanisms, while encouraging companies to assume broader social responsibilities.

(1) National AI Ethics Framework

By 2021, China had introduced a national AI Code of Ethics, outlining six fundamental principles for all AI activities: enhance human well-being; promote fairness and justice; protect privacy and security; ensure AI is controllable and trustworthy; uphold accountability; and cultivate ethical use.

Ethical requirements are increasingly baked into laws and regulations, offering detailed, actionable guidance to ensure compliant implementation.³ Key guiding principles for companies and individuals include:

- **Risk control:** Increase risk awareness, analyse potential AI development risks, carry out timely, systematic risk monitoring and evaluation, establish effective risk warning mechanisms, and improve the ability to manage and handle AI ethical risks.
- **Safety and transparency:** In algorithm design, implementation and application, improve transparency, explainability, comprehensibility, reliability and controllability. Boost AI system resilience, adaptability and anti-interference capability, and gradually make systems

verifiable, auditable, visible to supervision, traceable, predictable and trustworthy.

- **Avoid bias and discrimination:** In data collection and algorithm development, strengthen ethical review, consider differential demands, and avoid potential data and algorithm bias. Strive to achieve AI system inclusiveness, fairness and non-discrimination.
- **User protection:** Clearly inform users of the use of AI technology in products and services. Identify AI product and service functions and limitations, and safeguard users' rights to be informed and to consent. Provide simple, understandable solutions for users to choose or disengage from AI mode.
- **Responsible use:** Fully understand the applicable scope and negative impacts of AI products and services. Respect the rights of relevant parties to not use them and avoid improper use and abuse. Also, prevent unintentional harm to others' legitimate rights.

(2) AI research and development (R&D): Ethics by design

Companies developing AI technologies in China are expected to build ethics into their products from day one. Regulators emphasise “ethics by design”, meaning AI developers should address issues like bias, discrimination and privacy during the R&D phase.

On September 7, 2023, the Ministry of Science and Technology (MOST) and other agencies introduced the Trial Measures for Science and Technology Ethics Review (Ethics Review Measures), which mandate companies and institutions to conduct ethics reviews for research activities including: (i) sci-tech activities involving human beings as research participants, including the testing, investigation, observation and other research activities with human beings as objects, as well as the sci-tech activities utilising human biological samples and personal information data, etc.; (ii) sci-tech activities involving laboratory animals; and (iii) sci-tech activities that do not directly involve human beings or laboratory animals, but may pose challenges with ethical risks in terms of life health, ecological environment, public order and sustainable development, among others. Due to possible issues such as subject alienation, algorithmic discrimination, illusion and error, and responsibility assumption, the R&D of AI is, in principle, subject to ethics review.

As required by the Ethics Review Measures, companies engaging in AI research that involves sensitive fields of sci-tech ethics now have to establish an internal ethics review committee to evaluate projects for compliance with ethical norms. The membership of such committee must span multidisciplinary expertise: at least some members with AI/technical research backgrounds, plus experts in ethics, law, data security and, in autonomous regions, local-knowledge specialists to reflect regional contexts. To ensure independence and fairness, the committee must include gender diversity and at least one member external to the host organisation. According to public sources, various leading companies in China, including Alibaba, Tencent, Huawei, ByteDance and SenseTime, have established their internal ethics review committees to take charge of the ethics review matters related to AI governance.

(3) Sectoral adoption and guidance

As generative AI (Gen AI) tools gain traction across various industries in China, a growing number of regulators and professional associations are issuing specific ethical guidelines on the use of AI.

Industry/ Sector	Guidelines
Medical Academia	The Chinese Medical Association issued strict rules on the use of AI in academic writing. Gen AI tools or their outputs cannot be credited as authors, and AI must not be used to write substantive sections of academic articles. Violating these rules leads to outright rejection or retraction of the paper. Severe cases can lead to authors being blacklisted for two years.
Financial Institutions	In November 2023, the People's Bank of China issued the "Guidelines for Information Disclosure on the Financial Application of AI Algorithms", clarifying the principles, forms and contents of information disclosure, covering seven aspects of information disclosure including algorithm combination, logic, application, data, subject, change and audit.
Media Industry	The Translator Association of China released the country's first industry "Gen AI Application Guide" for translators. The guide warns that translators should continuously update professional knowledge and leverage AI only to augment – not override – human creativity and accuracy.
Education	The Ministry of Education has issued the "Guidelines for the Use of Gen AI in Primary and Secondary Schools" in May 2025, explicitly prohibiting students from directly copying AI-generated content as homework or exam answers and restricting the abuse of AI in creative tasks.

2. Gen AI Regulatory Requirements

China has moved swiftly to regulate Gen AI services ahead of other AI applications and fields due to the public uptake of ChatGPT-style tools and the risks of real-time misinformation and social instability. Chinese regulators recognised that Gen AI's ability to mass-produce text, images, audio and video could facilitate disinformation campaigns, deepfake propaganda and other content abuses with broad societal impact. The Interim Measures for the Administration of Generative Artificial Intelligence Services (Gen AI Measures) focus on compliance by Gen AI service providers, who will bear specific obligations for content governance and LLM security assessments, as well as data protection. Unlike the EU AI Act, the Gen AI Measures do not specify categorised compliance obligations corresponding to risk levels of AI systems and use cases.

General introduction

Under the Gen AI Measures, Gen AI technology refers to models and technologies that have the capability to generate content such as text, picture, voice or video, and Gen AI service refers to services generating text, picture, voice or video, etc. by using Gen AI technology. To strike a balance between the innovation and development of Gen AI technologies and their security, the R&D and internal use of Gen AI technology by companies and institutions within their entity is excluded from the applicability scope of the Gen AI Measures.

The Gen AI Measures primarily specify two main roles: "Gen AI service providers" *vis-à-vis* "Gen AI service users". China

does not separately define a "deployer" role – all responsibility falls on the service provider once the online services with Gen AI features/functions reach the public.

- Gen AI service providers must shoulder the full compliance burden and shall be responsible for lawful use of training data, protecting IP rights and personal data, and ensuring outputs meet legal and ethical standards. They must enter service agreements with users, inform users about lawful use and prevent minors' addiction.
- In contrast, Gen AI service users refer to simply the individuals that use the service and are treated as beneficiaries of protection. The Gen AI Measures do not impose elaborate obligations on end-users beyond adhering to lawful use, while users are explicitly given the right to lodge complaints if a service violates rules.

Multiple government bodies⁴ are empowered to strengthen oversight of Gen AI services in line with their respective mandates. Accordingly, the Gen AI Measures's enforcement is carried out through China's established regulatory apparatus under newly clarified rules. If a service provider flouts the Gen AI rules, authorities can issue warnings, require service suspension or model corrections, or impose fines under those statutes. In severe cases of "public security" breaches, the police may impose administrative punishment, and criminal charges can follow if a crime is constituted.

The Gen AI Measures assert extraterritorial reach by explicitly covering any service – regardless of where the provider is located – that is offered to the Chinese public. The CAC can also take technical measures (e.g., block or restrict access) against foreign Gen AI services that fail to comply with relevant rules.

Filing requirement related to specific algorithms

In China, certain Gen AI services must complete mandatory filings with the CAC before they can be launched and made available to the public. Article 17 of the Gen AI Measures further mandates that any externally facing Gen AI service with public-opinion attributes or social-mobilisation capabilities must undergo a formal security assessment and file with the provincial CAC (LLM Filing)⁵ and also complete the algorithm filing procedures under the Provisions on the Administration of Algorithm-generated Recommendations for Internet Information Services (Algorithm Filing). These are usually referred to as the "Dual Filing" requirement in the Gen AI regulatory regime.

- **LLM Filing:** Before rolling out any Gen AI products to the public, the Gen AI service provider must conduct a series of security assessments, prepare a security assessment report and complete the LLM Filing. Besides, the LLM Filing process also requires the filing entity to provide various information and materials related to the LLM to be filed, such as information related to main functions, target audience, applicable scenarios, training data situation, and service and safety prevention measures, relevant service agreements, the *corpus* annotation rules, a list of blocked keywords and the testing question set. The CAC's key focuses of the review include the following:
 - localisation on models and algorithms, fine-tuned data centre, chips and resources;
 - security of training data, including secure source, contents and annotation;
 - security of models, including content security, preciseness and reliability of generated contents;

formulation of a keywords library associated with security risks; a test question database on the generated contents; and a test question database on rejection for response; and

- security requirements at the go-live stage, such as service transparency, continuity and stability, and the rejection rate to inappropriate questions.

For Gen AI services provided based on third-party LLMs that have been filed (via API or other technical methods), they should implement a registration procedure at the provincial CAC. Compared with the LLM Filing process, the registration process requires fewer materials and is relatively simplified, consisting only of two major parts: self-assessment by the enterprise; and desktop review and testing by the local CAC.

- **Algorithm Filing:** An algorithm recommendation service provider with public opinion attributes or social mobilisation capabilities must submit the name of the service provider, service form, application field, algorithm type, algorithm self-assessment report, content to be published, and other information on the Internet Information Service Algorithm Filing System within 10 working days of the date of providing services and go through the filing procedures.

Transparency and disclosure

The Gen AI Measures mandate that Gen AI service providers must clearly define and publicly disclose the target audience, scenarios and purposes of their services, guiding users to use them rationally and avoid misuse. To facilitate regulatory inspections, Gen AI service providers are also required to supplement detailed explanations of the algorithm design, including the sources, scale, type, annotation rules and mechanisms of their training data during regulatory checks, as outlined in Article 19 of the Gen AI Measures.

According to the recommended national standard GB/T45654-2025 Cybersecurity Technology – Basic Security Requirements for Gen AI Service (which is used as the benchmark requirement and supporting document for the security assessment in the LLM Filing), the following information should be made public to users in easily accessible locations (e.g., the homepage and service agreement): (i) limitations of the service; (ii) summary of the models and algorithms used in the services; and (iii) the personal information collected and its use in the services.

Online content moderation

Under the Gen AI Measures and cyber content safety rules scattered in different laws and regulations (e.g., the Cybersecurity Law (CSL) and the Administrative Measures on Internet-based Information Services), Gen AI must not produce any material outlawed by law or regulations such as incitement to subvert state power, undermine the socialist system, endanger

national security, etc. Gen AI service providers should bear the primary responsibility for content safety and must promptly cease generation, stop distribution, remove offending content and retrain its models upon discovering any prohibited material. As market best practice, Gen AI service providers are suggested to implement multi-layered monitoring and review: automated algorithmic filters (e.g., keyword checks, image recognition); manual audits; and security screening of inputs and outputs.

Gen AI service providers should also provide an easy-to-use complaint channel, publish their handling procedures and timeframes, and, per Gen AI Measures, establish a robust complaints process with timely public feedback and acceptance of regulatory inspections. At the same time, end-users retain the right to escalate unresolved issues directly to regulatory bodies. In practice, as soon as a problematic output is detected, Gen AI service providers are required to stop generation, remove the content from circulation and retrain their models to prevent recurrence. They must then notify regulators of the incident, document all corrective actions, and – if users misuse the system for illegal purposes – issue warnings or suspend access in line with contractual and legal obligations. Many local CACs have sanctioned Gen AI service providers for generating prohibited content, citing a failure to fulfil its content-monitoring duties and ordering a service suspension.

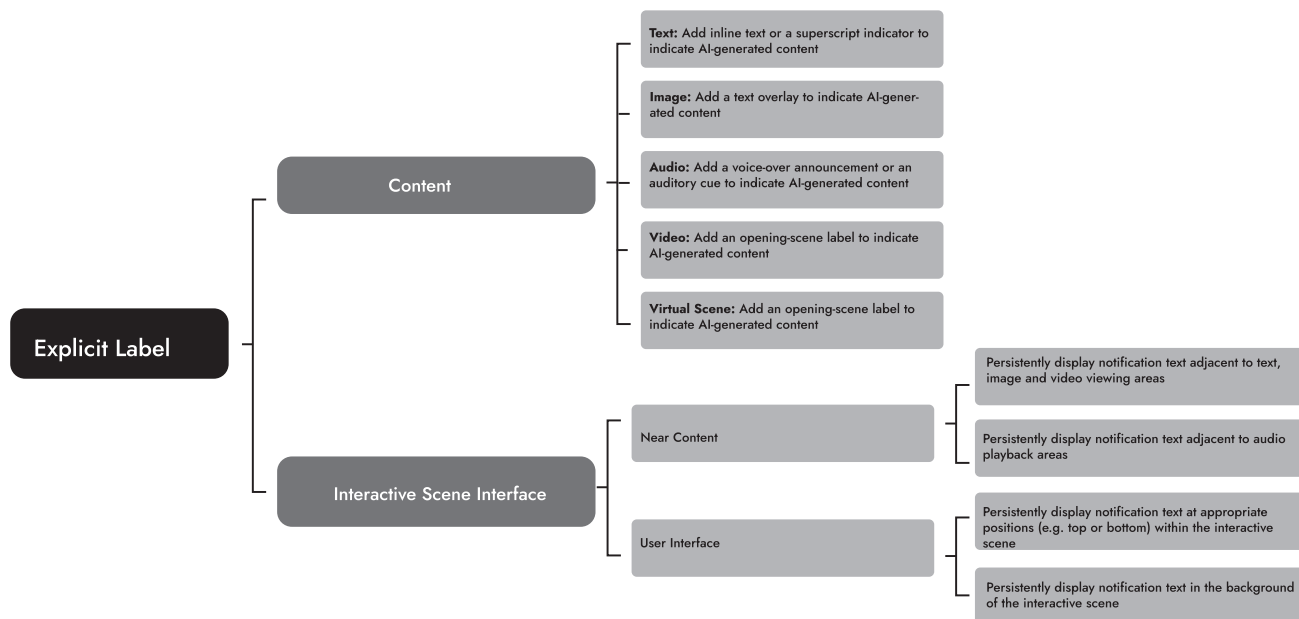
Although the Gen AI Measures do not provide detailed protocols for data breaches, existing regulatory frameworks under the CSL, the Data Security Law and the Personal Information Protection Law (PIPL) offer the necessary guidance. Failure to remediate promptly or serious violations will result in penalties.

Labelling requirements

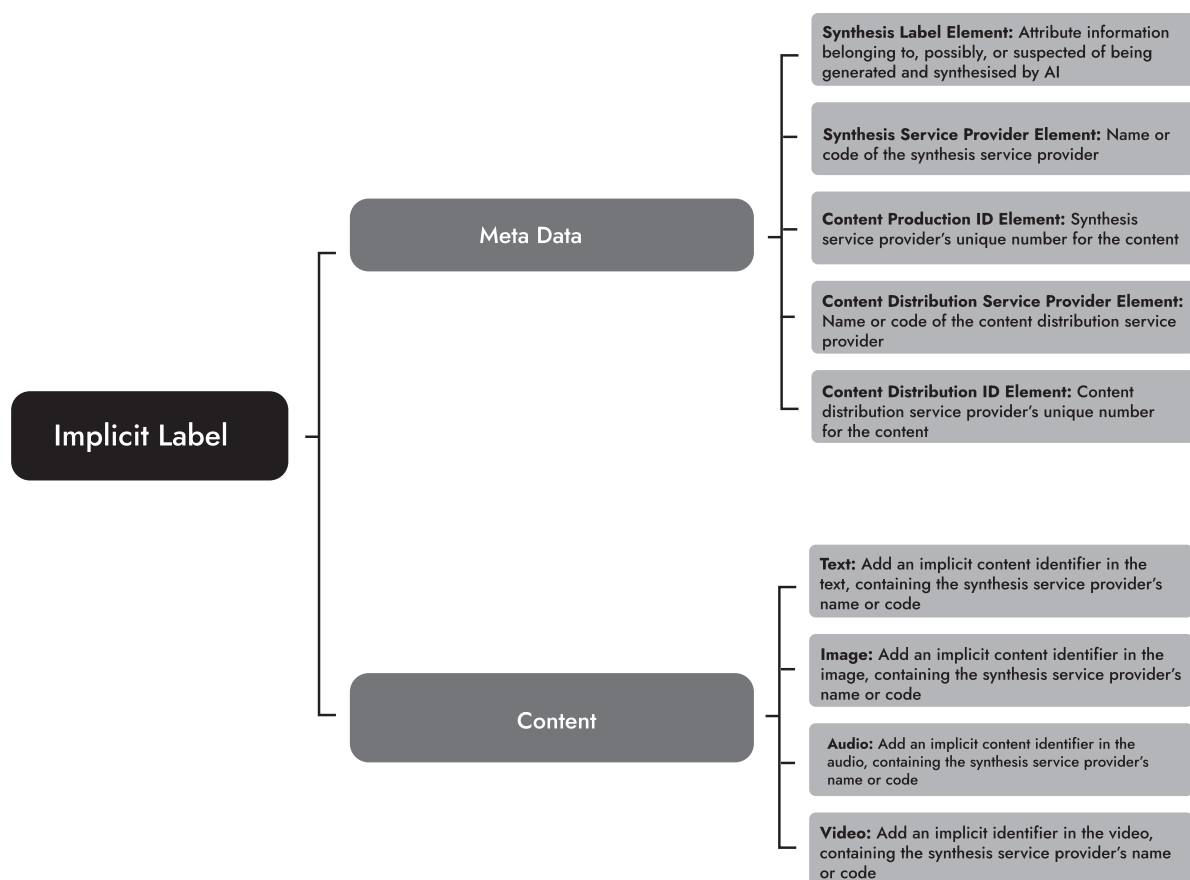
China requires clear labelling of AI-generated content to ensure users can distinguish machine-produced materials from human-created ones. The Provisions on the Administration of Deep Synthesis of Internet-Based Information Services require service providers to affix clear, visible labels on AI-generated images, audio and video. Non-compliance with labelling rules can trigger enforcement actions, including service suspension, fines or other administrative penalties.

In March 2025, the CAC and three other agencies jointly issued the Measures for the Labelling of Artificial Intelligence-Generated Content (Labelling Measures), alongside the mandatory national standard GB 45438-2025 Cybersecurity Technology – Labelling Method for Content Generated by AI, to require all network information service providers to clearly identify AI-generated content by September 1, 2025. Under the Labelling Measures, certain Gen AI service providers must apply both explicit labels and implicit labels.

Explicit Label Requirements

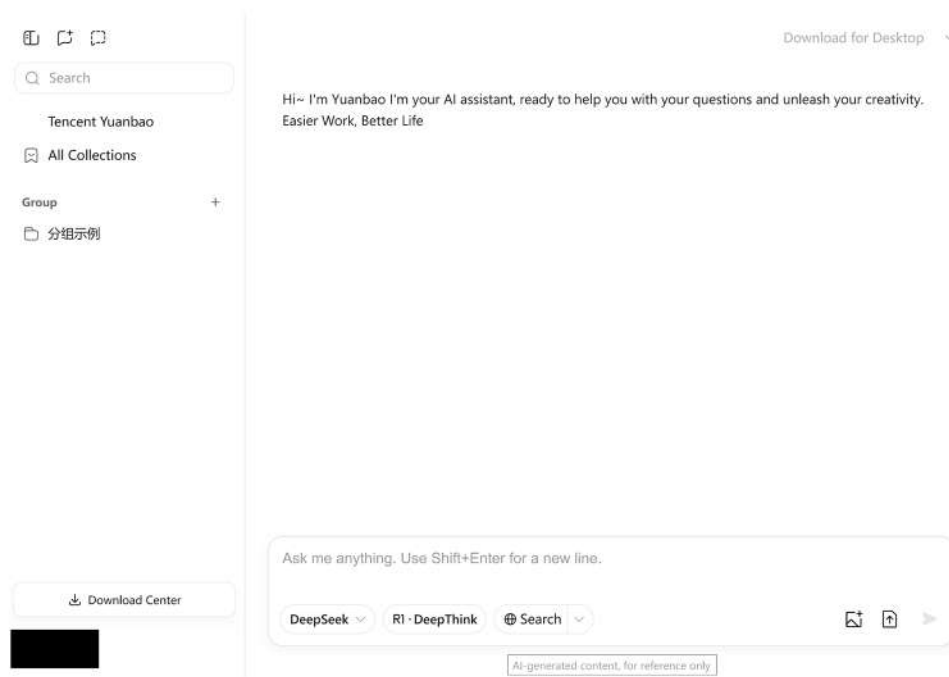


Implicit Label Requirements



Many Gen AI service providers are also strengthening transparency initiatives by labelling AI-generated content clearly to avoid public confusion. This is already mandated in the context of deepfakes-like algorithms (e.g., AI-altered videos must carry a conspicuous “AI synthetic” label) and now extends to generative text or images. They must also explain the mechanism of the AI services in the privacy policy or terms of use to obtain the consent of users.

services, and existing obligations under the CSL and the PIPL and other implementing laws and regulations remain valid. The primary obligations include notifying users of data processing (including but not limited to using user data for algorithm and LLM training), ensuring explainability, especially in healthcare, finance or other sensitive sectors, and secure prompt response to data subject requests for access, reproduction, correction, supplementation and deletion.



See “AI-generated content, for reference only” at the bottom of the image.



The image explicitly references AI-generated content.

Personal information protection

The Gen AI Measures do not introduce new rules concerning personal information protection in the context of Gen AI

When AI systems are offered to the public, especially for minors, explicit parental consent is required for children under 14, and age-verification mechanisms must be implemented.

3. AI Intersection with IP Protection

The National Intellectual Property Administration has led efforts streamlining AI patent examination and updating guidelines to clarify inventorship, authorship and liability. China has also seen a handful of illustrative cases in local courts that touch on AI-generated works and unfair-competition claims. Judicial practices and developments also shed light on how Gen AI technology interacts with IP rights protection.

Copyrights of AI-generated content

Chinese courts at the provincial level in various cases have ruled on how copyright applies to AI. In a landmark decision in November 2023, the Beijing Internet Court ruled that an image created by the user via an AI model can be a protectable “work” under copyright law. The court found that the human prompt-engineer had contributed enough creative input (selecting 150+ text prompts, adjusting parameters and refining outputs) to count as the author’s “intellectual achievement”, even though an AI model generated the final image. Thus, the user (plaintiff) was granted the copyright to the AI-generated image – explicitly rejecting the idea that the machine itself could be an author. Similar cases adjudicated

in Changshu (2024) and Wuhan (2025) reached consistent conclusions: when an author exercises “process control + originality of outcome” over generated works, the AI-generated content embodies their intellectual labour and thus merits protection.

In another case, the Guangzhou Internet Court issued China’s first known copyright-infringement judgment against a Gen AI service provider in February 2024. The court found that the AI system had unlawfully used copyrighted work in its output, holding the company liable for infringement. In December 2024, the Hangzhou Internet Court ruled that if a user distributes infringing content using a Low-Rank Adaptation model they created via the platform’s tools, and the platform has not discharged its duty of reasonable care, the platform will incur indirect liability for the user’s infringement. This aligns with China’s recent AI regulations: content generators are accountable for reproduced content. Together these cases indicate that Chinese courts will apply existing copyright laws to AI: if a human designer actively contributes to an AI output it may be protected, but unauthorised use of third-party copyrighted content can give rise to infringement liability.

Principle of fair use in AI training

The Gen AI Measures stipulates that Gen AI service providers should adopt training data and basic models from lawful sources and take effective measures to improve the quality of training data and to enhance the authenticity, accuracy, objectivity and diversity of training data. This means formulating detailed annotation protocols, conducting sampling-based audits of annotated samples, and training annotators on copyright compliance.

Although publicly available data is not strictly regulated from a cybersecurity standpoint, web scraping must adhere to intellectual property and data protection laws and must also comply with the target websites’ design and security protocols and measures. There has been a historical crackdown on web scraping, but recent interpretations of laws such as the CSL and PIPL now consider the specific type and nature of data, which means that not all web-scraping activities are illegal. However, ambiguities persist, notably regarding whether publicly disclosed personal information can legally be used for LLM training under the “reasonable scope” defined by China’s Civil Code.

Under China’s Copyright Law, traditional “fair use” exemptions (private study, quotation, news reporting, academic research) do not cover mass data ingestion and training, and no court precedent yet authorises unlicensed copying for AI and algorithm training.

Patentability of AI algorithm

China’s Patent Law defines an invention as a novel technical solution relating to a product or process. Under Article 25, “rules and methods for mental activity” – including pure mathematical methods and algorithms – are expressly excluded from patentability. Consequently, standalone AI algorithms or computer programs recorded in the media cannot be patented. However, when an AI algorithm is integrated into a concrete technical solution, it may meet the statutory requirements for a “technical solution” and thus be patentable.

4. Development Trend

Specific law enforcement campaign on AI

China has rapidly ramped up enforcement of its AI regulations. Local CACs have initiated numerous enforcement actions, penalising platforms for mass-generating prohibited content and for operating without having completed the required security assessments and filings. For instance, in 2024, Chongqing CAC shut down a ChatGPT-based service provided by Rongcheng Network Technology Studio of the Nanchuan District, where the online services used a LLM model that had not passed security assessment nor completed the LLM filing.

In April 2025, the CAC launched a three-month action plan called “Clear and Bright Crackdown on AI Technology Abuse”. The action is carried out in two phases, as follows:

- The first phase focuses on six key issues, including illegal AI products, the teaching and selling of such products, lax training material management, weak safety measures, the failure to implement content labelling requirements, and safety risks in key fields.
- The second phase targets seven major issues, such as using AI to create rumours, false information and pornographic content, impersonating others, engaging in online water army activities, and infringing on the rights of minors.

Typical enforcements and penalties are expected in the coming few months. Based on the regulatory focus of the first phase and several newly issued national standards, companies operating in China must prioritise robust compliance frameworks to mitigate legal and reputational risks in this rapidly maturing regulatory environment.

National and industrial standards are flourishing to polish regulatory rules

Aside from binding law and regulations, China’s formal AI standards ecosystem⁶ spans multiple facets of the AI domain, including data security and privacy protection, model evaluation and benchmarking, ethical and governance guidelines, interoperability protocols and risk-management frameworks. These supporting standards are expected to be provided in greater detail, translating abstract rules into practical checklists of compliance items that stakeholders can apply directly.

Besides, China’s AI alliances and think tanks have shifted from convening discussion to defining concrete rules and benchmarks that bridge policy and practice. The China Artificial Intelligence Industry Alliance launched the 2019 “Joint Pledge on AI Industry Self-Discipline”, setting ethics principles on safety, fairness and transparency that inform both regional guidelines and nascent draft regulations. Meanwhile, MIIT’s China Academy of Information and Communications Technology has produced authoritative white papers – such as the 2021 “Trustworthy AI” report – that crystallise criteria for robustness, explainability and risk control, and have driven the creation of pilot certification tools and performance benchmarks.

MNCs’ approach and adaption to China’s AI ecosystem

Chinese regulatory requirements mandate that Gen AI services offered to the public need to use LLM models that have been filed with Chinese regulators. Given the US–China technology

competition and geo-politics tension, US Gen AI technology providers are still navigating how to enter the China market. For compliance purposes, MNCs that plan to embed AI into consumer products and services will have to first seek and use Chinese Gen AI solutions. Besides, uncustomised overseas Gen AI models often fail to meet China's content regulations, risking security issues by generating non-compliant content. Practically speaking, local Gen AI players are able to offer cost-effective deployment solutions and high-performance AI models particularly after the emergence of DeepSeek. This means that many MNCs' governance approach and structure for AI applications and use cases in China will be different from the approach that they take for other jurisdictions.

Endnotes

- 1 Typical key policies include: "Internet+ AI" Three-Year Implementation Plan (2016); New Generation Artificial Intelligence Development Plan (2017); National AI Open Innovation Platforms (2019); AI Standardization Strategy (2020); AI Pilot Zones (2022); and "AI+" Initiative (2024).
- 2 https://www.mfa.gov.cn/mfa_eng/xw/fyrbt/fyrbt/202405/t20240530_11349822.html
- 3 Relevant laws and regulations include: Provisions on the Administration of Algorithm-generated Recommendations for Internet Information Services (2021); Provisions on the Administration of Deep Synthesis of Internet-Based Information Services (2022); Interim Measures for the Administration of Generative Artificial Intelligence Services (2023); Measures for the Labelling of Artificial Intelligence Generated Content (2025); and the following general laws: the Personal Information Protection Law (2021); the Data Security Law (2021); and the Civil Code (2017).
- 4 Such regulatory bodies include the CAC, the National Development and Reform Commission, the MOE, the MOST, the MIIT, the MPS, the National Radio and Television Administration, and their subordinate branches.
- 5 As of March 31, 2025, a total of 346 Gen AI services had completed the LLM filing.
- 6 In August 2020, the National New Generation AI Standardization Guidelines aimed to pre-research over 20 "key" standards (for general AI, niche tech, ethics, etc.) by 2021 and to launch an initial AI standards system by 2023 encompassing data, algorithms, systems, services and industry applications. Building on this, in May 2024, the CAC, the State Administration for Market Regulation and MIIT released the Action Plan to Develop Informatization Standards (2024–2027) to bolster standards for cutting-edge AI and related tech.



Kate Yin provides cyber security and data protection compliance services to various Chinese and foreign companies, including the establishment of compliance systems, responses to criminal and administrative law enforcement by governments, and responses to data breaches. Her clients include multinational companies and Chinese big companies from industries like e-commerce, big data AI, pharmaceutical and medical device, finance, consumer products, movie and television culture, manufacturing, consumer products and tourism. Ms. Yin's team has conducted deep research in legislation interpretation, and Ms. Yin participated in the formulation of important national standards such as guidance on the identification of important data as an expert of TC260.

Fangda Partners

27/F, North Tower, Beijing Kerry Centre
1 Guanghua Road, Chaoyang District, Beijing 100020
China

Tel: +86 10 5769 5617
Email: kate.yin@fangdalaw.com
LinkedIn: www.linkedin.com/in/kate-yin-esq-cfa-65985a



Gil Zhang specialises in privacy and data protection, cyber security and AI regulatory compliance. He has assisted companies in establishing data protection governance frameworks, global data protection strategies and compliance systems under the GDPR, as well as privacy and personal information protection laws in China and other Asia-Pacific countries. He also specialises in assisting clients to localise GDPR or FTC-mandated privacy protection systems to China and respond to enforcement actions by both domestic and foreign authorities. As the APAC general counsel, Mr. Zhang participated in BCR applications under the GDPR and the global implementation of GDPR, making him one of the few Chinese lawyers with international data protection experience.

Fangda Partners

24/F, HKRI Centre Two, HKRI Taikoo Hui
288 Shi Men Yi Road, Shanghai 200041
China

Tel: +86 21 6263 5922
Email: gil.zhang@fangdalaw.com
LinkedIn: www.linkedin.com/in/gil-zhang-76374421



Sherman Deng's practice focuses on data privacy and cybersecurity compliance. Sherman is currently representing both domestic and multinational clients in banking, finance, tourism, internet and manufacturing industries on data governance, incident response and cross-border data transfer matters. Before joining the firm, Sherman was a VP & Senior Counsel of Marriott International. In his seven years at the company, Sherman handled several high-profile data and cybersecurity incidents. He held a leadership role in preparing and implementing the company's cybersecurity-related compliance playbooks and policies, incident response plans, advising internal clients on MLPS, data localisation and cross-border data transfer projects, setting up cross-functional cybersecurity teams, building privacy and cybersecurity baselines, and managing other aspects of privacy lifecycle in China.

Fangda Partners

24/F, HKRI Centre Two, HKRI Taikoo Hui
288 Shi Men Yi Road, Shanghai 200041
China

Tel: +86 21 6263 5887
Email: sherman.deng@fangdalaw.com
LinkedIn: www.linkedin.com/in/sherman-deng-07010a12



Huihui Li is a specialist in privacy, data protection and cybersecurity compliance. He has assisted numerous companies with internal data compliance assessments, data compliance matters for overseas expansion, and data compliance due diligences (DCDDs) in investment and IPO projects. With extensive practical experience in cybersecurity and data protection under China's data protection law, Mr. Li focuses on data compliance assessment and analysis for data-intensive industries. He advises clients on general data compliance inquiries, internal system setup, security assessments and standard contractual clauses filing for cross-border data transfers, personal information protection impact assessments, and regulatory inquiries and law enforcement.

Fangda Partners

27/F, North Tower, Beijing Kerry Centre
1 Guanghua Road, Chaoyang District, Beijing 100020
China

Tel: +86 10 5769 5797
Email: huihui.li@fangdalaw.com
LinkedIn: www.linkedin.com/in/huihui-li-b08a3698

Founded in 1993, Fangda Partners is a full-service law firm advising on PRC and Hong Kong laws.

We have approximately 800 lawyers in our seven offices in Beijing, Guangzhou, Hong Kong, Nanjing, Shanghai, Shenzhen and Singapore. Our lawyers collaborate seamlessly across practice groups and locations to provide our clients with exceptional service, sophisticated advice and practical solutions founded on our legal expertise, sound knowledge of market practice, deep understanding of the industry landscape and proven ability to assist our clients to achieve their business objectives. We are the firm of choice for businesses requiring solutions to their most difficult and complex legal issues. Leading companies and financial

institutions in China and around the world turn to us for legal representation or counselling on their most significant legal and business challenges, whether transactions or disputes.

www.fangdalaw.com

FANGDA PARTNERS
方達律師事務所

The Increased Relevance for Companies of Data Collection of Racial and Ethnic Origins in the EU



Pierre Affagard



Laure Ekani

Clyde & Co LLP

I. Introduction

In the current international context, where diversity, equality and inclusion (**DEI**) policies are being scrutinised and even dismantled in some regions – particularly in the US with significant steps being engaged to ban DEI programmes within the federal government and pressure private companies to end similar initiatives – the need for robust measurement and data collection on origins and ethnicity in Europe is more pressing than ever and European Union (**EU**) regulations offer a variety of legal tools to do so.

This chapter outlines the legal framework surrounding the collection of data on origins and ethnicity, focusing on the applicable framework within the EU, with a particular attention to the French jurisdiction.

Although origins and ethnicity data have long been collected by public bodies and administration, there is still a disparity between Member States regarding the collection of such data by private actors like companies. This is at odds with companies being in demand of tools to monitor ethnic diversity in a context of increasing environmental, social and governance (**ESG**) legislation. Among these regulations is the Corporate Sustainability Reporting Directive (**CSRD**), published in December 2022.¹ It mandates companies across the EU to provide more transparent reporting on their ESG impact.² In the social responsibility branch, the CSRD includes mandatory reporting on labour practices, respect for human rights, equal treatment and opportunities for all, which includes measures against violence and harassment in the workplace, non-discrimination, and diversity and inclusion.³

In 2020, the EU Commission launched its EU anti-racism action plan (2020–2025), encouraging Member States to develop and adopt national legislations to combat racism and discrimination based on origins. Of relevance here, the Commission insisted on the need to collect reliable and comparable data on ethnic or racial origin for better informed policy choices. It observed disparities between Member States, some of which collected only data related to citizenship or country of birth.⁴ In response, the European Statistical Office launched a task force on “equality and non-discrimination statistics” in March 2024 to work with Member States and private companies to enhance the use of ethnic origins data and provide guidelines on the subject.⁵

In the UK, France and Hungary, national data protection authorities or national statistical offices have issued guidelines to support companies in their data collection efforts. France is an especially interesting case when it comes to measuring ethnic or origin-based diversity, as the French Data Protection Authority (**CNIL**) published early guidance on the

subject in 2005 and 2007, followed by a more comprehensive guide in 2012.⁶ The CNIL even updated these materials by releasing an up-to-date version aligned with the latest regulatory framework in July 2024.⁷

In response to this increased focus on non-discrimination based on origins in the workplace, national initiatives have been on the rise to enable willing companies to certify their commitment to tackling this issue.⁸ Such initiatives include certifications like the French Diversity Label (*Label Diversité* in French) created in 2008. This diversity monitoring tool certifies that a private or public organisation strives to implement non-discriminatory recruitment, integration and career-development processes.⁹ One of the first prerequisites for a company to obtain the Diversity Label is to conduct an assessment of its current situation in terms of equality, professional diversity, the fight against discrimination, and the promotion of diversity and inclusion.¹⁰ This assessment contains both qualitative and quantitative information on employees.

Quantitative tools are necessary means to design effective public policies to combat racism and racial discrimination. On a more micro-level, companies demand data to assess their level of diversity and inclusion in order to put forward corrective measures and comply with reporting obligations.

In this context, the legal framework applicable to the collection of data on origin and race may appear unclear or legally uncertain to some HR departments wishing to implement this type of measure. This is particularly the case in certain EU Member States where there is reluctance to collect such data out of fear that it may reinforce racial stereotypes or essentialise employees. For example, in France, there is a fairly widespread misconception that the collection of “ethnic statistics” is prohibited. However, at the European level, the General Data Protection Regulation (**GDPR**) provides a clear and harmonised framework that allows the collection of ethnic and origin-related data when the appropriate legal basis is used, and the rights of the data subject are protected.¹¹

II. Lack of Definition of Racial and Ethnic Origins

Before focusing on how data on ethnicity and origins is collected, it is necessary to look at the scope of these terms. The first notable point is that the GDPR does not define the terms “racial origin” or “ethnic origin”, even though they are mentioned in Article 9. The text simply specifies that “racial origin” does not imply a biological definition of race.¹²

A report commissioned by the EU Commission provides guidance in that respect.¹³ It reveals that, while most national legislation prohibit discrimination based on racial or ethnic

origins, the terms themselves are usually not defined in Member States' legislation.

The term "ethnic origin" refers more to a shared affiliation with a particular culture or geographic location. Ethnicity is thus a group situated between the notion of nation and that of clan. A legal definition that has been provided by a United Kingdom case law is that of a distinct community, distinguished by the sharing of one or more characteristics such as:

- (1) a long-shared history;
- (2) a cultural tradition of its own;
- (3) a common geographical origin or descent from a small number of common ancestors;
- (4) a common language;
- (5) a common literature;
- (6) a common religion; and
- (7) being a minority or being oppressed or a dominant group within a larger community.¹⁴

As for the term "racial origin", it refers to the concept of race. As mentioned above, the GDPR excludes the notion of biological race – that is, race understood as a group of people characterised by biological differences.

Unlike ethnicity, race is more of an assigned identity based on physical appearance and somatic traits.¹⁵ For sociologists, when utilising the concept of race, individuals are being characterised by their social position.¹⁶ It is an assignment that results from a social process, not a physiological fact.

The conclusions of the report drafted for the EU Commission are relevant to the collection of ethno-racial data:

*"Racial, ethnic and national origins are mutable grounds, comprising nationality, colour, descent, minority religion, minority language, minority culture and traditions. Together with foreign and immigrant, these characteristics constitute the most common proxies of racial or ethnic origin – most clearly borne out in the context of data collection on inequalities, which is decidedly based on these proxies."*¹⁷

This approach allows us to understand the concepts of racial or ethnic origins as fluid categories that can be objectified through a set of individually or jointly considered characteristics, which can then be measured during the data collection process.

III. Legal Prohibition with Exceptions Under the GDPR

Regulated like any other personal data

The collection of data on individuals' ethnicity and origins is currently governed by data protection law under the GDPR, which has been applicable since 25 May 2018. However, data protection is not a new legal concept. In France, for instance, the *Informatique et Libertés* law was enacted on 6 January 1978, and later the EU Data Protection Directive of 24 October 1995 was voted at a European level.¹⁸ Across all these legal instruments, data concerning ethnic or racial origin has consistently fallen within the scope of personal data law.¹⁹

The GDPR marked a major step forward by providing a directly applicable and harmonised legal framework across all EU Member States. Personal data is broadly defined as any information relating to an identified or identifiable natural person.²⁰ The Regulation clarifies that identification markers can include physical, social or cultural characteristics.

When an employer wishes to collect such data, they act as a "data controller" within the meaning of the GDPR and must do so in compliance with all mandatory legal safeguards, and upholding the rights of data subjects.

Because ethnicity and racial origin fall under the definition of personal data, their processing must rely on one of the legal bases listed in Article 6 GDPR.²¹ In the context of employment, the most relevant legal bases for processing ethno-racial data are explicit consent (Article 6(1)(a)) and legitimate interest (Article 6(1)(f)).²²

In July 2024, the CNIL issued guidelines measuring diversity in compliance with the GDPR.²³ One of its recommendations is to prefer legitimate interest over consent as a legal basis. The CNIL argues that legitimate interest offers stronger protection for employees' rights, particularly because freely given and informed consent is difficult to obtain in hierarchical employment relationships.²⁴

To use the legitimate interest basis, employers must clearly justify the legitimacy of the processing. For instance, they may argue that measuring diversity is necessary to comply with national laws on non-discrimination.²⁵

Applying the principle of purpose limitation

The principle of purpose limitation requires that data be collected for specified, explicit and legitimate purposes.²⁶ When collecting data on ethnic or racial origin, employers must frame the initiative within a broader strategy aimed at improving equality of opportunity in the workplace. Measurement alone does not provide sufficient justification.

For example, a diversity survey may serve to:

- detect potential discriminatory practices in recruitment or career advancement processes;
- identify inclusive HR practices that support equal treatment of employees; and/or
- track progress over time and evaluate the effectiveness of diversity initiatives, by repeating similar surveys at regular intervals.²⁷

Crucially, this type of data collection must never be used to make decisions about individual employees, but only to guide collective policy.

A prohibition with exceptions for special categories of data

The GDPR identifies nine special categories of personal data (also referred to as sensitive data) that warrant enhanced protection due to their potential impact on privacy. These include:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data;
- health data;
- data concerning sex life; and
- sexual orientation.²⁸

As discussed earlier, the concept of "data revealing ethnic or racial origin" should be interpreted broadly. For example, in 2022, the Belgian Data Protection Authority (APD) issued an opinion regarding a government project to monitor the number of immigrants or descendants of immigrants within civil servants.²⁹ It concluded that nationality, although objectively factual, could serve as a proxy for ethnicity, thereby falling within the scope of Article 9 GDPR.

The first paragraph of Article 9 GDPR sets out a general prohibition on the processing of special categories of data.

However, this prohibition is relativised in the following paragraph 2. In this context, the exceptions a), f) and j) are of particular importance.

According to Article 9(2)(a) GDPR, cases in which the data subject “has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject” are exempted from the prohibition in paragraph 1. EU law thus recognises the voluntary disclosure of sensitive data. This is the only appropriate exception for employers wishing to collect ethnic origin data. At the same time, however, the GDPR allows individual Member States to impose stricter requirements.³⁰

According to Article 9(2)(f), a further exception applies if “processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity”. In any case, this refers to those constellations in which statistics are intended to provide judicial proof of indirect discrimination or the adequacy of a positive measure.

Finally, Article 9(2)(j) allows the measuring of ethnic data for public interest, scientific or historical research purposes or for statistical purposes. This exception is used notably to process racial and ethnic origins data in national censuses.

Contrary to common assumptions in some Member States, ethnic and racial data are not prohibited under the GDPR without broad exceptions. Rather, they are treated with enhanced caution, like any other sensitive data. Data revealing ethnic or racial origin are not more sensitive than data revealing sexual orientation or trade union membership.

IV. Conditions and Obligations for Lawful Processing

This section outlines the key legal conditions and obligations under the GDPR that organisations must meet to ensure the lawful processing of special category data, such as origin-related information, in the context of workplace diversity surveys.

Obtaining explicit consent (Articles 6 and 7 GDPR)

The collection of special category data relating to origin must always be part of a voluntary process on the part of the employee.³¹ Non-participation in a survey must not lead to any form of sanction, and conversely, participation must not be incentivised. Respecting employees’ fundamental rights requires that participation in the survey remains entirely voluntary, with no obligation to respond.³²

However, relying on consent is not without legal complexity, particularly in the context of employment relationships. Indeed, it is more difficult in an employment setting to prove that the employee was not coerced into giving consent. The European Data Protection Board (EDPB), the EU authority responsible for ensuring consistent application of the GDPR, goes further by stating that it is unlikely that employees are in a position to freely refuse consent due to the dependent nature of the employment relationship.³³ Nevertheless, the EDPB acknowledges that in certain situations, an employer may lawfully obtain consent.³⁴

To ensure truly informed and freely given consent in the context of a diversity survey, the CNIL recommends involving a third party (a so-called “trusted third party”) to conduct the survey on behalf of the employer (see below).

Transparency and information duties (Article 13 GDPR)

Before collecting any data, the employer must inform employees, through a separate privacy notice containing several mandatory items.³⁵

This information must be presented in a concise, comprehensible and easily accessible format. Paper documentation, infographics or videos may help facilitate understanding. A multi-modal approach helps to achieve transparency.³⁶

To enhance transparency, it may also be appropriate (and in some cases mandatory) to involve the employee works council in the process.

Pseudonymisation of the processing

It is important to note that the GDPR does not apply to data that is anonymised at source and is therefore no longer considered as personal data. When data is collected through a process that ensures source anonymisation, the statistical operation falls outside the scope of the GDPR, and the obligations described in section III above do not apply (except for the requirement that participation remains voluntary).

To guarantee source anonymisation, the employer may provide a dedicated web page for the survey. Collecting employee names or email addresses must be strictly avoided.

However, anonymisation is not a prerequisite for lawful processing. If technical means or the organisation’s size do not permit full anonymisation, it is still possible to conduct non-anonymised surveys, provided that all appropriate GDPR safeguards are applied.

In all cases, it must be impossible to identify respondents retrospectively by cross-referencing answers. This ensures confidentiality during the processing and anonymisation when publishing the results of the study. This becomes more challenging in smaller organisations. To ensure anonymity of aggregated data, it is recommended to:

- use broad question categories (e.g., age ranges instead of exact ages, geographic areas instead of specific countries);
- remove names and first names from datasets during aggregation;
- delete any list of employees who responded to the survey;
- ensure aggregated statistics do not reference indirectly identifying information;
- set a pseudonymisation threshold below which data on small groups will not be published; and
- limit data retention to a few weeks or months following data aggregation.

Use of a trusted third party

Involving a third party to collect data on behalf of the employer to ensure the integrity of the survey process is essential. This trusted third party could be a law firm or a consulting firm specialising in diversity measurement.

The key point is that the employer must not have access to the raw data collected, nor know which employees responded or not. In this way, the use of a trusted third party guarantees the anonymisation of data *vis-à-vis* the employer, since the data will only be presented in aggregate form.

The trusted third party, responsible for administering the survey, ensures the security of the process, the confidentiality of the data, and helps guarantee that employees’ consent is freely given.

Carrying out a Data Protection Impact Assessment (DPIA) (Art. 35 GDPR)

Before beginning processing, it is essential for the employer to carry out a DPIA. Indeed, a DPIA is mandatory where the processing is “likely to result in a high risk to the rights and freedoms of natural persons”.³⁷ The EDPB specifically recommends conducting a DPIA where special category data under Article 9 GDPR is processed, or where the processing is carried out on a large scale.³⁸

Conducting a DPIA in the context of a diversity survey is not only a regulatory obligation; it is also best practice.³⁹ It is a key tool to ensure the processing does not unintentionally cause harm or expose the employer to legal or reputational risks.

V. The French Case: Clarifying the Legal Framework of Ethnic Data Collection

A data collection methodology regulated by a decision of the French Constitutional Council

In France, the Constitutional Council issued a decision in 2007 as part of a constitutional review of an immigration law, in which it established a legal framework for the collection of ethno-racial data. This decision was initially widely interpreted by the media, businesses and civil society as a blanket ban on data collection. In fact, the methodology defined by the Constitutional Council does not prohibit the collection of ethnic data but instead sets limits on the types of data that may be collected.

For context, a law aimed at combatting illegal immigration was passed in 2007, which included an amendment aimed to add a new exception to the existing list of derogations for the processing of special category data, specifically for “studies measuring diversity of origins”.

As a result of its constitutional review, the French Constitutional Council struck down this amendment.⁴⁰ In doing so, the Council also stated that surveys measuring diversity based on ethnic origin or race are prohibited under the principle of equality of all citizens before the law, as enshrined in Article 1 of the French Constitution.⁴¹ This decision gave rise to a strong presumption in France that all ethnic statistics are banned.

However, through subsequent comments by the Constitutional Council and decisions by the CNIL over the years up to the present day, it has become clear that it is indeed possible in France to measure ethnic or racial origin. What is prohibited is the establishment of an ethno-racial classification system.⁴² Below is a summary of what is and is not allowed in France today:

Type of data	Position of the Constitutional Council and CNIL	Example of questions
Objective data	Permitted	What was your nationality at birth? What is your country of birth? Where were your parents/grandparents born?

Type of data	Position of the Constitutional Council and CNIL	Example of questions
Subjective data, e.g. self-perception or perception by others	Permitted	How do you think others perceive you? <i>Note: the CNIL has not specifically ruled on this, but surveys conducted by public bodies have offered answers such as “Perceived as White/Black/Arab”, etc.</i> ⁴³
Ethno-racial classification system	Prohibited	Which of the following ethnic groups do you belong to (e.g., Asian/Latino-American/Arab)? What is your racial origin? What race do you identify with?

Examples of surveys conducted by private sector actors

In 2023, major French companies such as Carrefour and L’Oréal conducted ambitious, large-scale surveys measuring the diversity of origins among their employees.⁴⁴

The French Ministry of Labour even launched an online template survey to measure diversity and inclusion, with one section specifically focused on origins-based diversity.⁴⁵ This “Diversity and Inclusion Index” was developed in partnership with the CNIL and the French Human Rights Defender (*Défenseur des droits* in French) and is intended to serve as a secure and legally compliant measurement tool.

Some companies have already taken the lead, showing that it is possible to measure diversity of origins to engage in more targeted policymaking. The legal framework exists, the tools are available – now what is needed is a direction engaged by HR and diversity departments to establish these practices over time and make them common practice.

Endnotes

1 Directive (EU) 2022/2464 of the European Parliament and of the Council of 14 December 2022 amending Regulation (EU) 537/2014, Directive 2004/109/EC, Directive 2006/43/EC and Directive 2013/34/EU, as regards corporate sustainability reporting.

Directive of the European Parliament and of the Council amending Directives (EU) 2022/2464 and (EU) 2024/1760 as regards the dates from which Member States are to apply certain corporate sustainability reporting and due diligence requirements.

2 The CSRD applies progressively, depending on company size, to those meeting at least one of the following thresholds: more than 250 employees; €50 million in revenue; or €25 million in total assets. Please note the future Omnibus Directive may modify these thresholds.

3 Recital 49 and Article 29b of the CSRD.

4 “Accurate and comparable data is essential in enabling policy-makers and the public to assess the scale and nature of discrimination suffered and for designing, adapting, monitoring and evaluating policies. This requires disaggregating data by ethnic or racial origin. However, compared to data on other grounds of discrimination, such as sex, disability and age, such data is relatively scarce. Obstacles include problems in establishing a common methodology, with some

Member States collecting such data while others consciously avoid this approach. As a result, many surveys focus on the perception of discrimination or use proxies such as citizenship or country of birth. The collection of reliable and comparable data at [a] European and national level is an essential prerequisite for effective action.” (Communication From the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *A Union of equality: EU anti-racism action plan 2020–2025*, 18 September 2020.)

- 5 Report on the implementation of EU anti-racism action plan 2020–2025 and on national action plans against racism and discrimination, European Commission – Directorate-General for Justice and Consumers, 2024, p.9.
- 6 *Lutte contre les discriminations: les recommandations de la CNIL pour mesurer la diversité des origines*, 2005, CNIL.
Mesure de la diversité et protection des données personnelles, 2007, CNIL.
Mesurer pour progresser vers l'égalité des chances, 2012, CNIL.
- 7 *Enquêtes de mesure de la diversité au travail*, 2024, CNIL.
- 8 https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combating-discrimination/racism-and-xenophobia/eu-anti-racism-action-plan-2020-2025_en
- 9 <https://travail-emploi.gouv.fr/le-label-diversite#anchor-navigation-724>
- 10 https://cdn.afnor.org/download/documents/LBH000-CDC_Alliance_labels_LD_LEP_%2B50.pdf
- 11 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR).
- 12 “Those personal data should include personal data revealing racial or ethnic origin, whereby the use of the term ‘racial origin’ in this Regulation does not imply an acceptance by the Union of theories which attempt to determine the existence of separate human races.” (Recital 51 GDPR.)
- 13 “The meaning of racial or ethnic origin in EU law: between stereotypes and identities”, 2017, Lilla Farkas, Publication Office of the European Union.
- 14 *Mandla v Dowell Lee* [1983] 2 AC 548.
- 15 *Rapport du comité pour la mesure de la diversité et l'évaluation des discriminations (COMEDD)*, 2010, François Héran *et al.*, p.14.
- 16 *Le mot race – Cela existe* (1/2), 2019, Éric Fassin, AOC media.
- 17 “The meaning of racial or ethnic origin in EU law: between stereotypes and identities”, 2017, Lilla Farkas, Publication Office of the European Union.
- 18 Directive 95/46/EC of the European parliament and of the council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
- 19 Initially, the *Informatique et Libertés* law only mentioned processing of data on racial origins.
- 20 Article 4(1) GDPR.
- 21 Article 6 GDPR.
- 22 Consent is often seen as the most straightforward basis for processing ethnic data. The notion of consent will be analysed further in section IV.
In addition, the GDPR permits processing when it is in the legitimate interests pursued by the controller providing that:
 - It has a legitimate interest in collecting the data.
 - The processing of personal data is necessary to achieve this interest.
 - The fundamental rights and freedoms of the data subject do not override the legitimate interests.

- 23 *Projet de recommandation, Enquêtes de mesure de la diversité au travail*, 9 July 2024, CNIL.
- 24 See section IV above.
- 25 In France, the employer may invoke the need to comply with Law No. 2008-496 of 27 May 2008, which contains various provisions for the transposition of EU anti-discrimination law.
In Germany, the *Allgemeines Gleichbehandlungsgesetz* (AGG), or General Act on Equal Treatment of 18 August 2006, could be invoked to justify a legitimate interest.
- 26 Article 5(1)(b) GDPR.
- 27 *Mesurer pour progresser vers l'égalité des chances*, 2012, CNIL, p.36.
- 28 Article 9(1) GDPR.
- 29 Opinion no. 211/2022, 9 September 2022, APD.
- 30 In France, Article 9 GDPR is directly applicable without limitation under Article 6 of the local *Loi Informatiques et Libertés*.
On the contrary, in Spain, the consent of the data subject alone is not sufficient to lift the prohibition of processing of data identifying racial or ethnic origin (Article 9(1) of the *Ley Orgánica 3/2018*, of 5 December, *de Protección de Datos Personales y garantía de los derechos digitales*).
- 31 “*Erhebung von Antidiskriminierungsdaten in repräsentativen Wiederholungsbefragungen, Bestandsaufnahme und Entwicklungsmöglichkeiten*”, 2019, Dr. Anne-Luise Baumann, Vera Egenberger, Dr. Linda Supik report commissioned by the German Federal Anti-Discrimination Agency, p.33.
- 32 The employer must ensure that consent is freely given, specific, informed and explicit. The employee’s consent must be given specifically for the purpose of conducting a diversity or discrimination survey and must be documented either in writing or electronically, typically through a consent form.
In accordance with Article 7(3) GDPR, the controller must ensure that the employee can withdraw their consent at any time. Upon withdrawal of consent, the personal data concerning the individual must be deleted.
- 33 Guidelines 05/2020 on consent under Regulation 2016/679, 4 May 2020, EDPB, p.9.
- 34 For instance, German national data protection law considers the employee’s level of dependence in the employment relationship and the circumstances under which consent was given to assess whether such consent was freely given (Section 26(2) of the Federal Data Protection Act of 30 June 2017 (BDSG)).
- 35 Such items include:
 - the identity and contact details of the controller(s);
 - the contact details of the Data Protection Officer, if one is designated;
 - the purpose of the processing (e.g., measuring diversity of origin in the workplace);
 - the legal basis for processing and, if applicable, the legitimate interest pursued;
 - the right to withdraw consent at any time, where consent is the legal basis for processing;
 - the voluntary nature of participation and responses;
 - the recipients of the data;
 - the data retention period;
 - how to exercise rights such as access, rectification, erasure, etc.; and
 - the right to lodge a complaint with the CNIL.
- 36 For further guidance on the privacy notice, please refer to the Guidelines on transparency under Regulation 2016/679, adopted on 29 November 2017, as last revised and adopted on 11 April 2018, EDPB.
- 37 Article 35 GDPR.

- 38 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, 4 April 2017, EDPB.
- 39 A DPIA is designed to identify and control potential impacts on individuals’ rights and freedoms. It involves three key stages:
- analysing the specific characteristics and objectives of the data processing operation, along with any potential threats;
 - assessing the probability and potential consequences of those risks; and
 - introducing appropriate technical and organisational measures to minimise harm, secure the data and ensure the processing remains fully compliant with GDPR requirements.
- 40 Decision no. 2007-557DC, 15 November 2007, French Constitutional Council.
- 41 More specifically, Article 1§1 of the French Constitution provides that: *“France is an indivisible, secular, democratic, and social Republic. It ensures equality before the law for all citizens without distinction of origin, race, or religion. It respects all beliefs. Its organisation is decentralised.”*
- 42 À propos de la décision no. 2007-557 DC of 15 November 2007 sur la loi relative à la maîtrise de l’immigration, à l’intégration et à l’asile, 2008, 23e Cahier du Conseil constitutionnel.
- Decision no. 2023-133, 7 December 2023, CNIL.
- 43 *“Inégalités d’accès aux droits et discriminations en France”*, 2016, Défenseur des droits, La documentation française.
- 44 <https://www.carrefour.com/fr/news/2024/carrefour-brise-le-plafond-de-verre-et-sengage-pour-la-diversite-dorigine>
<https://www.loreal.com/-/media/project/loreal/brand-sites/corp/master/lcorp/3-commitments/for-the-people/respecting-human-rights/publication/rapport-diversite-equite--inclusion.pdf>
- 45 <https://www.egalite-femmes-hommes.gouv.fr/cp-retour-dexperience-index-diversite-et-inclusion-21-02-2022>



Pierre Affagard co-leads the data protection/cybersecurity practice at the Paris office at Clyde & Co, notably within the specific sectors of transportation and aviation, two areas in which the firm is widely recognised as a market leader. He is also a lecturer on data protection at Paris-Saclay University and acts for clients of the firm as an external DPO. Pierre is recommended by *The Legal 500* for Data Privacy and Data Protection and listed in *Best Lawyers* in France: Ones to Watch.

Pierre also developed a specific digital tool to measure ethnic statistics of employees, in full compliance with the restrictive French legal framework, which has already been used by political parties and organisations across France in their DEI efforts.

Clyde & Co LLP

18–20 rue Treilhارد
75008 Paris
France

Tel: +33 1 4443 8888

Email: pierre.affagard@clydeco.fr

LinkedIn: www.linkedin.com/in/pierre-affagard-842548ba



Laure Ekani's practice focuses on national and international insurance cases, particularly in the areas of product liability, industrial risks and professional indemnity. She has also developed a strong interest in workplace discrimination and the legal framework surrounding the collection of ethno-racial data by employers. Laure holds a Master's degree in Law from Sciences Po Paris and was admitted to the Paris Bar in 2024.

Laure has been working alongside Pierre Affagard to develop a specific digital tool to measure ethnic statistics of employees, in full compliance with the restrictive French legal framework, which has already been used by political parties and organisations across France in their DEI efforts.

Clyde & Co LLP

18–20 rue Treilhارد
75008 Paris
France

Tel: +33 1 4443 8888

Email: laure.ekani@clydeco.fr

LinkedIn: www.linkedin.com/in/laure-ekani-16521b158

Clyde & Co is a market-leading global law firm, focused on providing complete legal services to clients across their core sectors of insurance, transport, energy, infrastructure and trade. Clyde & Co has grown into one of the largest international law firms, helping clients navigate risk successfully.

Clyde & Co's Paris office was established in 1992 and is the oldest office of the firm in continental Europe. With decades of experience, the Paris office has a profound understanding of local and international legal landscapes, offering tailored solutions that meet the unique needs of clients.

Clyde & Co has developed a specific digital tool to measure ethnic statistics of employees/individuals in full compliance with the restrictive French legal framework. In this context, the firm has been assisting public institutions and political parties to help them in collecting and processing sensitive personal data to meet the growing demands and regulations around ESG and DEI.

Clyde & Co also has one of the largest dedicated global data breach teams, known as One, who have combined experience in handling 5,000 cyber events. This network is available 24/7 via global telephone hotlines and email, operating from all Clyde & Co offices across the globe. The firm has also built a range of innovative technology-led cyber products to enhance our cyber offering, which include ransomware response, BEC/account takeover response, active threat intelligence, data mining and AI DSAR tools.

www.clydeco.com

CLYDE & Co

Cloud Computing, Privacy Impact Assessments and Record-Keeping Regarding Data Protection in Japan

Chuo Sogo LPC



Yusaku Akasaki



Hiroki Minekawa



Ronald Kaloostian

1. Introduction

Data protection in Japan is governed by the Act on the Protection of Personal Information and its amendments (“APPI”), which was enacted in 2003 and fully came into force in 2005. Thereafter, the APPI was amended in 2015, 2020 and 2021. Currently, there are discussions regarding amendments to the APPI that may introduce an administrative penalty system in addition to the current fines, and establish systems for injunction claims and remedies for damages on behalf of consumer organisations.

The most notable change with the 2015 amendment, which fully came into force in 2017, was the establishment of the Personal Information Protection Commission (“PPC”). The extraterritorial application of the APPI was expanded as well.

The 2020 amendment fully came into effect in 2022 and included clarifications about personal information with regard to its ability to identify an individual, i.e. “person-related” rather than personal information, as well as pseudonymous information. It introduced a prohibition on a business operator handling personal information using personal information to potentially facilitate illegal or inappropriate acts. It also introduced the requirement that the APPI has to be reviewed every three years.

In this chapter we will address three specific topics under the APPI, as follows:

- privacy and security in cloud computing, focusing on a recent administrative case;
- Privacy Impact Assessments (“PIA”) in Japan; and
- records concerning the provision of personal data¹ to third parties in Japan.

2. Privacy and Security in Cloud Computing

Below we will discuss the evolving requirements for data protection in Japan for organisations using cloud computing. This could include the security and privacy challenges of storing and processing data in the cloud, and Japan’s regulations concerning cloud service providers and data centres.

In the context of information and communication technology, the term “cloud computing”, or simply “cloud”, refers to the provision of certain computing resources “as a Service” over the internet, or to such computing systems that are used to provide such services. There are many instances where a company stores and uses personal data of its customers or employees in the cloud; however, in some cases, this can cause a problem in relation to the regulation under the APPI. This section discusses the relationship between cloud usage

and the APPI, focusing on the regulations on the provision of personal data to third parties (as well as the issues related to the restrictions on the provision of personal data to third parties in foreign countries).

When a company stores and uses personal data of its customers or employees in the cloud, that personal data is transferred from the company to the cloud service provider. In view of the regulations imposed under Japanese law on the “provision” of personal data to third parties, a cloud service provider planning to operate cloud services in Japan may adopt one of the following three legal solutions: (1) obtaining the consent from the individuals; (2) entrustment; and (3) the so-called “cloud exception”.

1. Obtaining the consent from the individual

Japanese law allows the provision of personal data to third parties, provided that the consent from the individual to whom the personal data belongs (hereinafter the “individual”) is obtained (Article 27, paragraph (1) of the APPI). In reality, however, it may not always be easy for companies to comply with this provision, because obtaining consent from the individuals may not be straightforward when companies hold various types of personal data. For example, in the case where a company collects the personal data of its customer’s family, to store the collected data in the cloud it uses, it must obtain, directly or indirectly, the prior consent of each family member concerned, otherwise it cannot use the cloud for dealing with the collected data. As this is extremely impractical, the company may give up using the cloud after all.

It should also be noted that Japanese law puts an additional restriction on the provision of personal data to “third parties in foreign countries”² (Article 28 of the APPI). A foreign business operator (i.e., a business operator established in a foreign country) that receives personal data from a business operator handling personal information in Japan does not fall into the category of “third parties in foreign countries”, provided that the former is also a “business operator handling personal information” in Japan (Section 2-2 of *the Volume on Provision to a Third Party in a Foreign Country, the Guidelines for the Act on the Protection of Personal Information* (the “APPI Guidelines”)), because Japanese law applies to business operators handling personal information in Japan. On the other hand, however, it is also provided that whether a foreign business operator qualifies as a “business operator handling personal information” under Japanese law is determined on a case-by-case basis, taking into consideration the actual state of its business in Japan,³ from which it can be said that the criteria for such determination are yet to be clearly defined. If a foreign

business operator takes “appropriate and reasonable means” (Article 16 of the APPI enforcement rules) in appropriate ways, the “restriction on the provision of personal data to third parties in foreign countries” does not apply to the foreign business operator. However, this is also determined on a case-by-case basis (Section 4-1 of the APPI Guidelines).

Accordingly, it can be said that, for foreign business operators planning to operate a cloud business in Japan, it should be hard to establish such a business based on the self-procurement of individual consent and hence they should adopt other solutions, namely entrustment or cloud exception (discussed below).

2. Entrustment

If the act of storing and using personal data in the cloud can be deemed to constitute the “entrustment” of personal data-handling to a cloud service provider, it does not fall under third-party provision (Article 27, paragraph (5), item (i) of the APPI). “Entrustment” of personal data-handling means that “a ‘business operator handling personal information’ is having another party handle personal data by any form or type of contract” (GL3-4-4 of the General Rules of the APPI), and is considered one of the grounds for exceptions to third-party provision regulations under Japanese law. As explained below, there are cases where it is difficult to adopt the solution of “cloud exception” and the only available solution is “entrustment”. Please be advised that if the cloud service provider is located in “foreign countries” under the PPC, the “entrustment” theory cannot be used.

The entrustor has an obligation to supervise the trustee (Article 25 of the APPI). Hence, a business operating cloud services in Japan is subject to the supervision by the entrustor (i.e., the cloud user). The entrustor is required to supervise the trustee to ensure that the trustee takes security control measures equivalent to those the entrustor should take under Article 23 of the APPI; cloud users may thus demand strict supervision of cloud service providers.

However, if, at the request of a cloud user, a cloud service provider discloses its server configuration details to the cloud user or allows the cloud user to enter into its data centre without careful consideration, the cloud service provider risks losing trust from other cloud users. On the other hand, the cloud service provider may not refuse all of the user’s demands on supervision, due to the strict obligation of supervision imposed on the user.

The PPC closely monitors compliance with such obligation. For example, in the Notice it issued on March 25, 2024, the PPC called for the attention of business operators handling personal information by reminding them of the key consideration for employing a cloud service provider, as follows:

- Before selecting cloud service providers and services, fully understand and confirm not only the functions and support system of the target services but also the security measures included in the services.
- Clearly document the content of necessary and appropriate security control measures (including the roles and responsibilities in the handling of personal data) agreed with the cloud service provider concerning the handling of personal data as objectively as possible in the form of terms and conditions or a contract (Q5-8 of *FAQs on the APPI Guidelines*).
- Review the statuses of the security measures and the security control measures of the service being used, by, for example, obtaining regular reports from the cloud service provider.

In this context, it can be said that an extremely careful judgment must be made regarding the extent to which a cloud service provider should accept the cloud users’ demands on supervision.

There are hardly any examples of administrative advice on the level of supervision required for cloud use, and the PPC does not have any explicit judgment criteria. Such being the situation, consulting a law firm specialised in the APPI may be essential for those engaged in the cloud businesses.

3. Cloud exception

The “cloud exception” is a concept that in a third-party provision of personal data, no consent thereto is required in the cases where the contract stipulates that the recipient of the data shall not “handle the received personal data” because such cases do not constitute provision of personal data from a company to a cloud service provider (Q7-53 *op. cit.*). Such a concept of excluding an act of storing in and using the cloud from the scope of “provision” is unique to Japan, as by contrast, the General Data Protection Regulation includes the act of storing personal information *per se* in the definition of the term “processing”.

It is said that to “not handle personal data” refers to the cases where the contract stipulates that the cloud service provider shall not handle the personal data stored on the server and where appropriate access control is in place (Q&A7-53 *op. cit.*). As mentioned above, the “cloud exception” is a concept unique to Japan, and the conditions for applying the “cloud exception” are not clear, with many issues remaining unresolved also in the APPI. For example, while it is required that the contract contains a provision of “no handling of personal data”, in practice, virtually no business operators stipulate “no handling of personal data” in any case. It is thus very difficult to determine what kind of cases are appropriate for stipulating disclosure of personal data.

In recent years, there was a case where the PPC denied the applicability of the cloud exception. It is a case involving information leakage at MKSystem Corporation (“MK”), a provider of business systems services dedicated to certified social insurance and labour consultants. The PPC denied the applicability of the cloud exception to that case on the grounds that MK had been in fact a cloud service provider entrusted with the handling of personal data, rather than a provider “not handling personal data”, which is recognised as a case that put a brake on the mass-producing of cloud exception cases.

Specifically, the PPC denied the applicability of the cloud exception for reasons including the following:

- The terms of use stipulated specific cases where MK was allowed to use personal data pertaining to the clients of the certified social insurance and labour consultants or others using the service.
- MK had a maintenance ID that provided MK with access to the personal data in the system where no technical access control or other measures were taken to prevent MK’s unauthorised handling of the data.

It is said that until this decision was presented, there were many cases that were easily configured as cloud exceptions.

In the event where the applicability of the “cloud exception” is denied, the relevant business operator handling personal information and the cloud service provider may face the risk of having to drastically reorganise their cloud business operation. Hence, failure to comply with Japanese law can be a major blow to both business operators handling personal information and cloud service providers. However,

the option of “entrustment” is not quite user-friendly in view of the supervisory obligations. After all, for foreign business operators planning to operate a cloud business in Japan, use of the last option, namely the “cloud exception”, should be the best solution.

On the other hand, as can be seen from the fact that the PPC also denies, in general terms, the applicability of the “cloud exception” to cases involving processing of personal data including editing and analysing (“Response from the competent authority to the request for consideration, FY2022, No. 307”), it is difficult to rely on a legal position to the deployment of SaaS (i.e., software and services made available over the internet) in Japan. Consequently, the option of “entrustment” should also be legally positioned as a secondary solution, because relying solely on the option of “cloud exception” is too risky. In the future, as the PPC’s administrative advice examples accumulate, the legal positioning of cloud use should become clearer. Until then, at least for the time being, a safe way to operate may be to take a two-tier approach with the “cloud exception” as the primary solution and “entrustment” as the secondary solution.

3 PIA

Are PIA required under Japanese law? If so, in what circumstances and what should they include?

Under Japanese law, PIA is not considered a mandatory obligation for business operators handling personal information. However, when handling personal information, it is crucial to incorporate the protection of individual rights and interests, including personal information protection, into the design stage of business operations. PIA, a risk management method that evaluates potential impacts in advance to reduce or avoid risks of infringing on privacy and other individual rights and interests during the initiation or modification of businesses involving the collection of personal information, is encouraged as a voluntary initiative. In 2021, the PPC published a report titled “Promotion of PIA Initiatives – Points to Consider in Line with the Significance and Implementation Procedures of PIA”, which discusses the significance and specific methods of PIA.

The significance and effects of implementing PIA include the following:

1. Gaining trust from stakeholders, including consumers: It serves as proof of appropriate measures taken to comply with laws and reduce risks, contributing to social credibility. Additionally, by publishing results, it fulfils accountability, enhances transparency and helps eliminate information asymmetry between consumers and business operators handling personal information.
2. Reducing total business costs: Necessary measures can be taken before deciding on significant system investments or business discontinuation, ultimately controlling total business costs.
3. Improving governance, including employee education: Employees become aware, and management can grasp the handling status of personal information, thereby improving governance.

An example of specific implementation procedures includes:

- “Preparation”, which involves comprehensive and broad information collection and organisation, such as system development and confirmation of personal information flows, after considering whether to implement PIA.
- “Risk Identification and Evaluation”, where evaluators specifically identify and assess risks related to personal

information handling and identify significant risks and matters requiring action based on the preparation.

- “Risk Reduction”, where designers and others formulate and execute specific measures and plans to reduce the risks identified and evaluated.

In practice, the approach varies depending on the scale, nature and content of personal information, and it is important for business operators handling personal information to consider the optimal method themselves. The results of PIA implementation should be compiled into a report, not only for reporting to the management of the business operators handling personal information but also for external publication from the perspective of accountability and transparency to stakeholders, including consumers. In such cases, it is effective to create a summary and publish it concisely and understandably, rather than detailing the implementation results.

The report may include the flow of personal information handling, the scope of PIA implementation within that flow, implementation methods, identified risks, evaluation results of those risks, and countermeasures. Although PIA is not a legal obligation in Japan, it is promoted as a voluntary initiative, and considering that some countries have made it a legal obligation, it is expected that more businesses will implement it in the future. When implementing, it is important not to do so aimlessly but to fully understand its significance and ensure appropriate effects, implementing PIA content suitable for each business.

There is no requirement to consult the data protection authority before processing if a PIA indicates high risk.

4 Records Concerning the Provision of Personal Data to Third Parties

Are organisations required to maintain internal records of their processing activities? If so, what details must be recorded and who can access them?

Yes, business operators handling personal information must create records concerning the date of provision of personal data to third parties and the name or title of the third party when providing or receiving personal data from third parties. The principle is to create records promptly each time personal data is exchanged, but there is an exception where records can be created collectively instead of individually when personal data is exchanged continuously or repeatedly with a specific business within a certain period.

Additionally, when entering into a contract for the provision of goods or services to the person and providing personal data of the contracting party to a third party in the course of fulfilling the contract, it is possible to track the distribution of personal data using the contract or other documents created at the time of provision, and these documents can serve as records.

Records must include the following items:

When providing to third parties with consent:

1. “Name or title and address of the third party, and in the case of a juridical person, the name of its representative.”
2. “Name of the person identified by the personal data and other matters sufficient to specify the person.”
3. “Items of the personal data.”
4. “Statement of obtaining the person’s consent.”

When receiving with consent:

1. “Name or title and address of the third party, and in the case of a juridical person, the name of its representative.”

2. “Background of the third party’s acquisition of the personal data.”
3. “Name of the person identified by the personal data and other matters sufficient to specify the person.”
4. “Items of the personal data.”
5. “Statement of obtaining the person’s consent.”

In certain cases, it is possible to omit record items. Regarding the recorded third-party provision records, if a disclosure request is made by the person, it is necessary to disclose the information to the requesting parties without delay. However, in the following cases, it is exceptionally permissible not to disclose all or part of the records:

1. Cases where disclosure is likely to harm the life, body, property, or other rights or interests of the person or a third party.
2. Cases where disclosure is likely to seriously impede the proper execution of the business of the business operator handling personal information.
3. Cases where disclosure violates other laws and regulations.

5 Conclusion

Above we discussed three important topics regarding data protection in Japan. First, as the PPC addresses more cases with respect to cloud computing, we expect the scope of the “cloud exception” to become clearer. However, as the MK case indicates, a provider of business systems services over the internet may be considered to have been entrusted with the handling of personal data, in which case the option of “entrustment” should also be legally positioned as a secondary solution. Thus, it may be prudent for companies to follow a two-tier approach for the time being with the “cloud exception” as the primary solution and “entrustment” as the secondary solution.

Second, in Japan, although PIA is not a legal obligation, it is encouraged as a voluntary initiative to reduce or avoid risks of infringing on privacy and other individual rights and

interests. When implementing, it is important to fully understand its significance, implementing PIA content suitable for each business.

Finally, in Japan, business operators handling personal information must create records concerning the date of provision of personal data to third parties and the name or title of the third party when providing or receiving personal data from third parties. Although the principle is to create records promptly each time personal data is exchanged, there is an exception where records can be created collectively instead of individually when personal data is exchanged continuously or repeatedly with a specific business within a certain period. If the data subject requests the business operator to disclose its own personal data, in general the business operator shall disclose the personal data to the data subject. Notwithstanding this obligation, there are exceptional cases in which it is permissible not to disclose all or part of the records (e.g., likely to harm the life, body, property, or other rights or interests of the person or a third party).

Endnotes

- 1 We use the terms “personal data” and “personal information”. To be precise, the definitions are different under the APPI, but we do not distinguish them in this chapter.
- 2 However, Article 28 excludes countries that are prescribed by Order of the PPC as having a personal data protection system recognised as being of a similar standard to that of Japan from the scope of “foreign countries”. For example, as of the time of writing this chapter, EEA countries (EU countries, Iceland, Liechtenstein and Norway) and the UK do not fall under the category of “foreign countries”.
- 3 See Q12-5 of *FAQs on the APPI Guidelines*. Since the location of the server is not a criterion for determination, if a U.S. company’s server is located in an EU country and a Japanese business operator handling personal information stores personal data in the cloud on that server, it is deemed a transfer to a third party in the U.S. (i.e., subject to Article 28 of the APPI).



Yusaku Akasaki handles a wide range of consultations for corporate clients and has extensive (foreign and domestic) experience, particularly in corporate law, M&A, labour and employment matters, competition law and data protection law.

Leveraging his study abroad experiences in the United States and the Middle East, Yusaku frequently provides support and advice to clients on cross-border commercial transactions, data protection matters and M&A.

Chuo Sogo LPC

Osaka Dojimahama Tower 15th Floor
1-1-27 Dojimahama, Kita-ku
Osaka, 530-0004
Japan

Tel: +81 6 6676 8834

Email: akasaki_y@clo.gr.jp

LinkedIn: www.linkedin.com/in/yusaku-akasaki-856379a5



Hiroki Minekawa has completed one year of legal training, and has worked as a lawyer at Chuo Sogo LPC for two years. He particularly works on cases related to IT law and Finance law.

He offers practical advice about the Act on the Protection of Personal Information in Japan and also handles a number of general litigation cases.

Chuo Sogo LPC

Osaka Dojimahama Tower 15th Floor
1-1-27 Dojimahama, Kita-ku
Osaka, 530-0004
Japan

Tel: +81 6 6676 8834

Email: minekawa_h@clo.gr.jp

URL: www.clo.jp/english/lawyers/688



Ronald Kaloostian worked in the in-house IP department of a major Japanese innovator pharmaceutical company for over 11 years. He specialised in IP licensing, IP due diligence, joint research collaborations with US universities, strategic biopharma alliances and spin out of new companies with novel technologies and inventions. Ron joined Chuo Sogo LPC in 2023 and practises in the areas of IP, M&A, International Transactions, Data Privacy and Cybersecurity, and Global Compliance.

Chuo Sogo LPC

Hibiya Kokusai Building, 18th Floor
2-2-3 Uchisaiwaicho, Chiyoda-ku
Tokyo 100-0011
Japan

Tel: +81 3 3539 1877

Email: ronald_k@clo.gr.jp

LinkedIn: www.linkedin.com/in/ronald-kaloostian-700b627

From the time the firm established its first office in 1968, it has built a solid business foundation by faithfully responding to the diverse needs of its clients.

We are confident that as a team of specialised lawyers we can render competent legal services in a broad range of legal fields by leveraging our expertise accumulated over many years as well as drawing on our long experience in resolving complex legal issues in and out of court.

We have strengthened ties with law firms in foreign countries, and have become an active member of a worldwide network of overseas law firms.

By taking advantage of such international cooperative systems, we can effectively take care of international issues that clients may face.

Our one-stop legal services are also supported by collaborations with domestic certified public accountants, certified tax accountants and patent attorneys.

www.clo.jp



Australia

Nyman Gibson Miralis



Darren Pham



Phillip Salakas



Harry Sultan

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

In Australia, there is data protection legislation at a state, territory and federal level. At the federal level, the principal data protection legislation is the *Privacy Act 1988* (Cth) (**'Privacy Act'**), including the Australian Privacy Principles (**'APPs'**).

1.2 Is there any other general legislation that impacts data protection?

The *Do Not Call Register Act 2006* (Cth) (**'DNCRA'**) and *Spam Act 2003* (Cth) (**'Spam Act'**) set out limits to direct marketing activities. At the state and territory level, the legislation concerned with data protection includes, for example: the *Information Privacy Act 2014* (Australian Capital Territory); the *Privacy and Personal Information Protection Act 1998* (New South Wales, **'NSW'**); the *Information Privacy Act 2009* (Queensland, **'QLD'**); the *Personal Information and Protection Act 2004* (Tasmania); and the *Privacy and Data Protection Act 2014* (Victoria, **'VIC'**).

1.3 Is there any sector-specific legislation that impacts data protection?

Privacy issues specific to the telecommunications sector are contained within the *Telecommunications Act 1997* (Cth) (**'Telecommunications Act'**) and the *Telecommunications (Interception and Access) Act 1979* (Cth).

Information related to healthcare is further protected under the *My Health Records ('MHR') Act 2012* (Cth) and the *Healthcare Identifiers Act 2010* (Cth). A multiplicity of state legislation also exists in relation to the protection of health-based privacy.

Businesses in industries such as financial services and gambling must comply with the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) and the Anti-Money Laundering and Counter-Terrorism Financing Rules.

The *Security of Critical Infrastructure Act 2018* (Cth) applies to organisations that own or operate (or hold a direct interest in) assets in a range of sectors, including communications, energy, defence, financial services, transport, data processing or storage, supermarket/grocery supply chains, health and medical, education and space.¹

Other examples of state, territory and federal legislation that relate to specific data protection or activities include:

the *Criminal Code Act 1995* (Cth); the *National Health Act 1953* (Cth); the *Telecommunications Act*; the *Health Records Act 2001* (VIC); the *Health Records*; and the *Workplace Surveillance Act 2005* (NSW).²

1.4 What authority(ies) are responsible for data protection?

The Office of the Australian Information Commissioner (**'OAIC'**) is an independent statutory agency which is endowed with functions under the *Privacy Act* and other legislation relating to data protection.

The Australian Communications and Media Authority (**'ACMA'**) is the regulatory authority charged with enforcing the *DNCRA* and *Spam Act*, as well as having other functions under the *Telecommunications Act*.

The Commonwealth Attorney-General's Department has responsibilities under the *Telecommunications (Interception and Access) Act 1974* (Cth). In coordination with the OAIC, the National Health and Medical Research Council has issued several binding guidelines in respect of privacy concerning health-related information.

The Australian Transaction Reports and Analysis Centre is the agency responsible for administering the *Anti-Money Laundering and Counter-Terrorism Financing Act*.

Various state and territory authorities also regulate privacy law issues in those jurisdictions. These include: the ACT Information Privacy Commissioner; the NSW Information and Privacy Commission; the Office of the Information Commissioner for the Northern Territory; the QLD Office of the Information Commissioner; the South Australian Privacy Committee; the Tasmanian Ombudsman; the Office of the Victorian Information Commissioner; and the Office of the Information Commissioner for Western Australia.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

■ "Personal Data"

The analogous term used in the *Privacy Act* is 'personal information'. This is defined in section 6 of the *Privacy Act* to mean information or an opinion about an identified individual or an individual who is reasonably identifiable:

- whether the information or opinion is true or not; and

- whether the information or opinion is recorded in a material form or not.

■ “Processing”

The Privacy Act does not refer to ‘processing’ but regulates ‘dealing with’ personal information in terms of ‘use’ and ‘disclosure’ (see Part 3 of the APPs). Though both terms are not defined in the Privacy Act, the OAIC indicates that:

- ‘Use’ means the handling or undertaking of activity in respect of information within its effective control.
- ‘Disclose’ means to make information accessible to others outside the entity and to release subsequent handling of such information from the entity’s control. The state of mind or intentions of the recipient does not affect the act of disclosure. Further, there will be a disclosure in these circumstances even where the information is already known to the recipient.

■ “Controller”

The Privacy Act does not refer to ‘controllers’ but rather covers the information-processing activities of APP entities. An APP entity is defined to be an agency or organisation.

An ‘organisation’ is defined to be:

- an individual (including a sole trader);
- a body corporate;
- a partnership;
- any other unincorporated association; or
- a trust,

unless it is a small business operator, registered political party, state or territory authority or a prescribed instrumentality of a state.

‘Agency’ refers to Australian Government (and Norfolk Island Government) agencies but does not include state and territory agencies. An ‘agency’ is defined to be:

- a Minister;
- a Department;
- a body (whether incorporated or not) or a tribunal, established or appointed for a public purpose by or under a Commonwealth enactment, not being:
 - an incorporated company, society or association; or
 - an organisation that is registered under the Fair Work (Registered Organisations) Act 2009 or a branch of such an organisation;
- a body established or appointed by the Governor-General or by a Minister, other than by or under a Commonwealth enactment;
- a person holding or performing the duties of an office established by or under, or an appointment made under, a Commonwealth enactment, other than a person who, by virtue of holding that office, is the Secretary of a Department;
- a person holding or performing the duties of an appointment, being an appointment made by the Governor-General or by a Minister, other than under a Commonwealth enactment;
- a federal court;
- the Australian Federal Police;
- a Norfolk Island agency;
- the nominated Australian Government Health Service company;
- an eligible hearing service provider; or
- the service operator under the Healthcare Identifiers Act 2010.

A person shall not be taken to be an agency merely because the person is the holder of, or performs the duties of, certain offices, such as a judicial office or of an office of magistrate.

■ “Processor”

Whilst the term ‘processor’ is not used in the Privacy Act, the APPs naturally apply to APP entities to the extent that they hold personal information. According to the OAIC, this is sufficiently broad to encompass outsourced serviced providers which, for example, in Europe might be considered ‘processors’.

■ “Data Subject”

The Privacy Act regulates the processing of personal information about individuals, defined in section 6 to mean natural persons.

■ “Sensitive Personal Data”/“Special Categories of Personal Data”

The Privacy Act defines ‘sensitive information’ as information or an opinion about an individual’s:

- racial or ethnic origin;
- political opinions;
- membership of a political association;
- religious beliefs or affiliations;
- philosophical beliefs;
- membership of a professional or trade association;
- membership of a trade union;
- sexual orientation or practices; or
- criminal record,

that is also personal information or:

- health information about an individual;
- genetic information about an individual that is not otherwise health information;
- biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
- biometric templates.

■ “Data Breach”

For the purposes of the Privacy Act, an ‘eligible data breach’ occurs where there is unauthorised access to, or unauthorised disclosure of, certain information and a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates.

■ “Collects”

As defined in section 6 of the Privacy Act, an entity collects personal information only if this is done for inclusion in a record or generally available publication.

■ “De-identified”

Personal information is de-identified if it is no longer about an identified individual or an individual who is reasonably identifiable. De-identification involves two steps. The first is the removal of direct identifiers. The second is taking one or both of the following additional steps:

- the removal or alteration of other information that could potentially be used to re-identify an individual; and/or
- the use of controls and safeguards in the data access environment to prevent re-identification.

■ “Employee Record”

The Privacy Act defines an ‘employee record’ as a record of personal information relating to the employment of the employee. Examples of personal information relating to the employment of the employee are health information about the employee and personal information about all or any of the following:

- the engagement, training, disciplining or resignation of the employee;
- the termination of the employment of the employee;

- the terms and conditions of employment of the employee;
- the employee's personal and emergency contact details;
- the employee's performance or conduct;
- the employee's hours of employment;
- the employee's salary or wages;
- the employee's membership of a professional or trade association;
- the employee's trade union membership;
- the employee's recreation, long service, sick, personal, maternity, paternity or other leave; or
- the employee's taxation, banking or superannuation affairs.
- **"Holds"**
An entity holds personal information if the entity has possession or control of a record that contains the personal information.
- **"Identification Information"**
Identification information about an individual means:
 - the individual's full name;
 - an alias or previous name of the individual;
 - the individual's date of birth;
 - the individual's sex;
 - the individual's current or last known address and two previous addresses (if any);
 - the name of the individual's current or last known employer; or
 - if the individual holds a driver's licence – the individual's driver's licence number.
- **"Record"**
A record includes a document or an electronic or other device. It does not, however, include:
 - generally available public information;
 - anything kept in a library, art gallery or museum for the purposes of reference, study or exhibition;
 - Commonwealth records in the open access period;
 - records in the care of the National Archives of Australia;
 - documents placed in the memorial collection of the Australian War Memorial; or
 - letters or articles transmitted by post.

3 Territorial and Material Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

Section 5B(1A) of the Privacy Act extends its application to acts done, or practice engaged in, outside Australia and the external territories by an organisation or small business operator with an Australian link. An organisation or small business operator has an Australian link if the organisation or operator is:

- an Australian citizen;
- a person whose continued presence in Australia is not subject to a limitation as to time imposed by law;
- a partnership formed in Australia or an external territory;
- a trust created in Australia or an external territory;
- a body corporate incorporated in Australia or an external territory; or
- an unincorporated association that has its central management and control in Australia or an external territory.

An organisation or small business operator also has an Australian link if all of the following apply:

- the organisation or operator is not described in subsection 2; and
- the organisation or operator carries on business in Australia or an external territory.

However, section 6A of the Privacy Act dictates that the APPs will not be breached by any conduct external to Australia that is required by an applicable foreign law.

3.2 Do the data protection laws in your jurisdiction carve out certain processing activities from their material scope?

Pursuant to section 16 of the Privacy Act, the APPs do not apply to the collection, holding, use or disclosure of personal information by an individual, or personal information held by an individual, only for the purposes of, or in connection with, his/her personal, family or household affairs.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

■ Transparency

The object of APP 1 is to ensure that APP entities manage personal information in an open and transparent way. An APP entity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions or activities that:

- will ensure that the entity complies with the APPs and a registered APP code (if any) that binds the entity; and
- will enable the entity to deal with inquiries or complaints from individuals about the entity's compliance with the APPs or such a code.

An APP entity must have a clearly expressed and up-to-date policy ('**APP privacy policy**') about the management of personal information by the entity. An APP entity must also take such steps as are reasonable in the circumstances to make its APP privacy policy available free of charge and in such form as is appropriate.

■ Lawful basis for processing

Broadly speaking, the lawful basis upon which an entity may process personal data is the consent of the individual. However, the majority of the APPs contain limitations or extensions relating to the application of Commonwealth laws, records and/or agreements. APP 3.5 specifies that personal information may only be collected by lawful and fair means.

■ Purpose limitation

Pursuant to APP 6, where an entity has collected personal information for a particular person, that information cannot then be used or disclosed for any further purpose other than with consent of the individual. This is limited, however, by certain defined exceptions, such as where the individual would hold a reasonable expectation of disclosure, where disclosure is required/authorised by a court or tribunal, or where a certain permitted health situation exists (See APPs 6.2 and 6.3).

■ Data minimisation

The APPs address data minimisation in a piecemeal approach, combining a prohibition on reallocation of the

purpose for holding information without consent (APP 6), limiting the collection of information to that which is reasonably necessary for the function in question (APP 3), and mandating destruction/de-identification where no purpose for use or disclosure of the information remains (APP 11).

■ **Proportionality**

Pursuant to APP 3, an APP entity may only collect personal information to the extent that it is reasonably necessary for, or directly related to, one or more of the entity's functions or activities. For sensitive information, collection further requires the individual's consent.

■ **Retention**

APP 11.2 requires an APP entity to take such steps as are reasonable in the circumstances to destroy or de-identify personal information it holds about an individual when:

- the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under this Schedule;
- the information is not contained in a Commonwealth record; and
- the entity is not required by or under an Australian law or a court/tribunal order to retain the information.

■ **Accuracy**

APP 10.1 requires an APP entity to take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity collects is accurate, up-to-date and complete. Pursuant to APP 10.2, an APP entity must also take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.

■ **Dealing with unsolicited personal information**

Where an APP entity receives unsolicited personal information, APP 4 requires that the entity must, within a reasonable period after receiving the information, determine whether the entity could have collected the information under APP 3 if the entity had solicited the information. If the APP entity determines that the entity could not have collected the personal information, and the information is not contained in a Commonwealth record, the entity must, as soon as practicable, but only if it is lawful and reasonable to do so, destroy the information or ensure that the information is deidentified.

■ **Crossborder disclosure of personal information**

Unless authorised, entities that intend to disclose personal information in a cross-border context must, pursuant to APP 8, take reasonable steps to ensure that the foreign entity receiving such information complies with the APPs. This is subject to exceptions, such as where that foreign entity is subject to a similar privacy regime under foreign law, or the information is being disclosed pursuant to a treaty obligation.

■ **Government-related identifiers**

APP 9 prohibits (with certain exceptions) the adoption, use or disclosure of government-related identifiers for individuals, by non-government organisations.

■ **Security of personal information**

Pursuant to APP 11, if an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

■ **Right of access to (copies of) data/information about processing**

Pursuant to APP 12, if an APP entity holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information. The APP entity is not required to give the individual access to the personal information in certain circumstances set out in APP 12.3, including where giving access would be unlawful, have an unreasonable impact on the privacy of other individuals, or would pose a serious threat to the life, health or safety of any individual, or to public health or public safety.

■ **Right to rectification of errors**

Pursuant to APP 13, if an APP entity holds personal information about an individual and either:

- the entity is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out-of-date, incomplete, irrelevant or misleading; or
- the individual requests the entity to correct the information,

the entity must take such steps (if any) as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up-to-date, complete, relevant and not misleading.

■ **Right to deletion/right to be forgotten**

Where an APP entity holds personal information about an individual and the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity, APP 11.2 requires that the APP entity take reasonable steps to destroy the information or to ensure that it is deidentified. This is subject to the information not being contained in a Commonwealth record and the APP entity not being required by or under an Australian law, or a court/tribunal order, to retain the information.

■ **Right to object to processing**

In practice, an individual's power to restrict processing of their personal information is limited to their initial withholding of consent to the collection of such information. APP 2 permits individuals to use a pseudonym or not identify themselves when dealing with an APP entity (unless required/permitted by law, or if this would be impractical). Additionally, APP 5 requires that individuals be notified before (or as soon as practicable after) their personal information is collected, thereby giving them the opportunity to object to such collection by disengaging with the entity.

■ **Right to restrict processing**

Whilst the APPs impose certain restrictions on how personal information can be dealt with (such as those relating to the purpose for which information is held (APPs 3 and 6)), there is no right bestowed on individuals to restrict the manner with which their information is dealt. Any such control held by an individual is largely relinquished upon the initial giving of consent to its collection.

■ **Right to data portability**

A broad right to data portability does not presently exist under Australian law (although, pursuant to APP 12,

individuals can request a copy of their personal information held by an APP entity). However, the Australian Government is actively moving to progressively legislate this right – to be known as ‘consumer data right’ (‘CDR’) – into Australian law. The Australian Competition and Consumer Commission will be the lead regulator of CDR.

- **Right to withdraw consent**

The OAIC’s APP guidelines indicate that consent must be current and specific. This includes enabling an individual to withdraw their consent at any time, which should be an easy and accessible process. Once an individual has withdrawn consent, an APP entity can no longer rely on that past consent for any future use or disclosure of the individual’s personal information. Individuals should be made aware of the potential implications of withdrawing consent, such as no longer being able to access a service.

- **Right to object to marketing**

APPs 7.2 and 7.3 require APP entities using personal information to engage in direct marketing to provide a simple means by which individuals may easily request to not receive such communications. If such a request is made, the entity must cease direct marketing to the individual.

- **Right protecting against solely automated decision-making and profiling**

A broad right addressing the right of individuals to be informed regarding the existence of solely automated decision-making and profiling does not presently exist under Australian law.

- **Right to complain to the relevant data protection authority(ies)**

The OAIC is empowered to receive individual complaints about the handling of personal information. It can also recognise external dispute-resolution schemes that handle particular privacy-related complaints. For example, if an individual’s privacy complaint is about a bank in Australia, he or she can contact the Australian Financial Complaints Authority.

- **Right to anonymity**

Pursuant to APP 2, individuals must have the option of not identifying themselves or using a pseudonym when dealing with APP entities, unless that entity is required/authorised by law to deal with individuals who have identified themselves, or if dealing with non-identified individuals would be impracticable.

- **Right to notification**

Pursuant to APP 5, APP entities must notify individuals about the collection of their personal information before, or as soon as practicable after, it occurs.

5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

There is no express provision addressing data subjects having the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress. However, a representative complaint may be lodged under section 36 of the Privacy Act if the conditions of section 38 of the Privacy Act are satisfied.

6 Children’s Personal Data

6.1 What additional obligations apply to the processing of children’s personal data?

According to the OAIC, an organisation or agency handling the

personal information of an individual under the age of 18 must decide if the individual has the capacity to consent on a case-by-case basis. As a general rule, an individual under the age of 18 has the capacity to consent if they have the maturity to understand what is being proposed. If they lack maturity, it may be appropriate for a parent or guardian to consent on their behalf.

If it is not practical for an organisation or agency to assess the capacity of individuals on a case-by-case basis, as a general rule, an organisation or agency may assume an individual over the age of 15 has capacity, unless they are unsure.

7 Registration Formalities and Prior Approval

7.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

There is no legal obligation on businesses to register with or notify the OAIC or any other bodies in relation to their data-processing activities in general. Specific obligations arise when eligible data breaches occur, as detailed in section 16. However, the OAIC has issued guidance to assist APP entities to prepare responses to any such breaches.

There is an option to ‘opt-in’ for small businesses and not-for-profits to good privacy practices and be covered under the Privacy Act. Allowing for increase in consumer confidence and trust.

7.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

This is not applicable in Australia – please see response to question 7.1.

7.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

This is not applicable in Australia – please see response to question 7.1.

7.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

This is not applicable in Australia – please see response to question 7.1.

7.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

This is not applicable in Australia – please see response to question 7.1.

7.6 What are the sanctions for failure to register/notify where required?

This is not applicable in Australia – please see response to question 7.1.

7.7 What is the fee per registration/notification (if applicable)?

This is not applicable in Australia – please see response to question 7.1.

7.8 How frequently must registrations/notifications be renewed (if applicable)?

This is not applicable in Australia – please see response to question 7.1.

7.9 Is any prior approval required from the data protection regulator?

This is not applicable in Australia – please see response to question 7.1.

7.10 Can the registration/notification be completed online?

This is not applicable in Australia – please see response to question 7.1.

7.11 Is there a publicly available list of completed registrations/notifications?

This is not applicable in Australia – please see response to question 7.1.

7.12 How long does a typical registration/notification process take?

This is not applicable in Australia – please see response to question 7.1.

8 Appointment of a Data Protection Officer

8.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

Currently, in Australia, organisations are not required to appoint a Data Protection Officer. However, the Information Commissioner has issued guidance recommending that organisations appoint a Data Protection Officer as good practice.³

A Data Protection Officer in Australia is known as a Privacy Officer and whilst not mandated by law, it is arguably essential in practice to comply with APP 1.2.⁴ The *Privacy Act Review Report 2022*, spoke directly about the role of Privacy Officers in Australia: ‘The role should be recognised as an important

one within the entity. For larger organisations, it would be expected that the Privacy Officer would be at a senior level that reports to the highest management level.’⁵

8.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

Currently, in Australia, there are no formal sanctions for failing to appoint a Data Protection Officer or Privacy Officer.

8.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

In Australia, there is no specific legislation that outlines protections or safeguards for Privacy Officers or Data Protection Officers during their course of employment. However, according to best practice within government agencies, a Privacy Officer will not be held personally responsible for non-compliance with the Australian Government Agency Privacy Code.⁶

8.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

According to best industry practice by government agencies, a Data Protection Officer or Privacy Officer may be appointed to act for a group of companies or a public authority. However, it is understood that depending on an organisations size, functions and structure, an organisation may decide to appoint more than one Data Protection Officer/Privacy Officer.⁷

8.5 Please describe any specific qualifications for the Data Protection Officer required by law.

Under Australian legislation, there are no prescribed academic or working background qualifications to be a Data Protection Officer or Privacy Officer.⁸

8.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

The OAIC recommends that Privacy Officers regularly report to their entity’s governance body. In relation to best practice for government agencies, the OAIC recommends that Privacy Contact Officers should be at least at the executive level and:

- participate in the development of initiatives with a privacy impact;
- advise on the application of the Privacy Act;
- handle or supervise the handling of privacy complaints;
- train staff in relation to relevant aspects of the Privacy Act; and
- be the primary contact for the OAIC.⁹

8.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

No, registration/notification is not required.

8.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

No. The OAIC requires privacy policies to be high-level documents that are not expected to contain specific details about all the entity's practices, procedures and systems relating to management of personal data.

9 Appointment of Processors

9.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

As the APPs do not specifically refer to 'processors', this is not strictly the case. However, although the Privacy Act and APPs do not refer explicitly to processors, the OAIC's view is that APP entities that are outsourced service providers holding personal information, even if not controlling it as such, must comply with this legal regime.

Where the processor is located overseas, the regulation of foreign information transfer is detailed in APP 8 and the OAIC has provided guidance for data processors or controllers with an establishment in the EU to ensure they are GDPR compliant.¹⁰

9.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

Although not applicable, entering such agreements remains best practice. In the context of cross-border disclosure, the OAIC under APP 8, recommends that such contracts cover:

- the type of personal information and purpose for its disclosure;
- a requirement that the recipient of the information complies with the APPs;
- the complaints-handling process; and
- a requirement as to the implementation of a data-breach response plan.

10 Marketing

10.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

APP 7.1 imposes a general prohibition on the use of personal information for the purpose of direct marketing.¹¹ This does not apply where the organisation provides a simple means through which the individual can opt-out of the marketing and:

- the information was collected in circumstances that would give rise to reasonable expectation of the information being used in such marketing; or
- the individual has consented to the receipt of such marketing.¹²

10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

The APPs do not speak specifically to the business-to-business context. However, it could be argued that these restrictions do in fact apply in the business-to-business context.

10.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

The national DNCRA prohibits most unsolicited telemarketing calls and fax messages to numbers placed on a national Do Not Call Register, without the consent of the person/organisation being contacted.

The Spam Act proscribes the sending of most unsolicited and non-consensual electronic messages. Some exceptions to this prohibition are electronic messages by government bodies, political parties and charities.¹³

10.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?

The Spam Act regulates the sending of commercial electronic messages with 'an Australian link'. This covers messages that:

- originate in Australia;
- were sent, or authorised by, an individual/organisation physically present in Australia, or with central management and control in Australia, when the message was sent;
- were accessed by a computer, server or device that is located in Australia;
- is connected to an electronic account-holder that is either an individual physically present in Australia or an organisation carrying on business or activities in Australia when the message is accessed; or
- if unable to be delivered due to the non-existence of a delivery address would, had the address existed, reasonably likely have been accessed using a computer, server or device located in Australia.¹⁴

The DNCRA concerns telephone calls and fax messages sent to 'an Australian number'. This means numbers that are specified in the plan set out in the Telecommunications Act and for use in connection with the supply of carriage services to the public in Australia. Section 9 of the DNCRA also expressly extends the legislation's application to acts carried out outside Australia's territory. Under APP 7.6(e), individuals may request to be advised of the source of their personal information used or disclosed in relation to direct marketing.

10.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

The ACMA is responsible for enforcing and investigating breaches of the Spam Act. The ACMA is a robust organisation which actively enforces breaches of marketing restrictions in Australia.

A recent case where ACMA litigated against V Marketing Australia Pty Ltd (In Liq) (no 4) [2025] FCA 287, saw the Federal Court imposing penalties totalling \$1.5 million against V Marketing and its sole director. The ACMA had uncovered that from the period of 1 March 2017 to 30 September 2017, V Marketing had made 553,630 telemarketing calls on behalf of Balaska Pty Ltd (solar business) to numbers on the Do Not Call Register, and that V Marketing also made an additional 548,688 calls to numbers on the same registry on behalf of Your Choice Solar Pty Ltd from 1 February 2018 to 28 September 2018.

10.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

In Australia, APP 3.6 governs the solicitation of personal information. It states that an entity 'solicits' personal information 'if the entity requests another entity to provide the personal information, or to provide a kind of information in which that personal information is included'. This request may be made to an agency, organisation, individual or a small business operator on behalf of another. A 'request' under this principle is an active step taken by an entity to collect personal information and may not involve direct communication between the entity and an individual.¹⁵

Arguably, APP 3.6 to some extent prevents the purchasing of marketing lists from third parties. The essence of this rule is that personal information should be collected directly from the individual concerned ('direct collection'), rather than from third parties or other sources.¹⁶

However, for organisations, the exception to the rule requiring direct collection is that it would be unreasonable or impracticable to do so.¹⁷ APP 3.65 stipulates that determining whether it is unreasonable or impracticable to collect personal information solely from the individual depends on specific circumstances. Relevant considerations include the individual's expectation of direct collection, the sensitivity of the information, potential jeopardy to the collection purpose or data integrity, privacy risks from alternate sources, and the time and cost of direct collection.¹⁸

APP 3.68 provides an example where an agency may collect personal information from a third party, such as when an individual consents to one agency disclosing their information to another agency. Regarding consent, as discussed in paragraph 3.23 and Chapter B, it can be express or implied, must be voluntary, informed, current and specific, and the individual must possess the capacity to consent.¹⁹

10.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Breaches of the DNCRA may result in corporate liability for civil penalties up to \$2.1 million, and individual liability for up to \$420,000 per day. This will depend on the number of breaches and the history of the actor.²⁰ Compensation can also be ordered where a victim has suffered loss or damage.

This penalty regime (and maximum sanctions) is largely mirrored in respect of the Spam Act.

Additionally, the Privacy Act contains numerous provisions addressing the payment of civil penalties, fines and compensation to victims.

11 Cookies

11.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

There is no specific legal regime that applies to cookies. Whilst the information collected through the use of cookies is often generalised, where it rises to the level of enabling identification of an individual, the use of cookies will be subject to the APPs.

However, there is new technology that combines cookie information, which is called data aggregation, and may be subject to legislative restrictions.

11.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

Whilst the APPs do not (in theory) apply differently to different cookies, the OAIC has issued public guidance about their distinctive operations and how individuals can adjust their browsing preferences accordingly.²¹

11.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

To date, the OAIC has not done so.

11.4 What are the maximum penalties for breaches of applicable cookie restrictions?

This is not applicable in Australia.

12 Restrictions on International Data Transfers

12.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

The transfer of personal information to jurisdictions outside Australia is governed by APP 8. APP 8.1 requires that entities must take 'reasonable steps' to ensure that a foreign recipient of personal information complies with the APPs. According to APP 8.2, however, this is not necessary where:

- it is reasonably believed that the recipient is subject to a law, or binding scheme, that bears overall substantial similarity to the APPs and the individual can take action to enforce such protections;
- the entity has obtained the individual's consent to the foreign disclosure;
- the foreign disclosure is required or authorised by Australian law;
- a permitted general situation (such as to lessen or prevent serious health and safety risks, or to take appropriate action in relation to suspected serious misconduct) applies;
- such disclosure is required by a government agency under an agreement to which Australia is a party; or
- the disclosure is by a government agency and relates to foreign law-enforcement activities.

‘The Attorney General’s *Privacy Act Report 2022* proposed certain amendments to be made to APP 8 to apply to de-identified datasets. The Report also recommends prohibiting APP entities from re-identifying de-identified information received from a third party and introducing a new criminal offence for “malicious” re-identification intended to harm or cause illegitimate benefit.’²²

12.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

The OAIC espouses an expectation that, to take the necessary reasonable steps, entities transferring personal information to foreign recipients will enter into enforceable contracts requiring compliance with the APPs. Under section 16C of the Privacy Act, if an entity has disclosed personal information on the basis of a belief that the foreign recipient will be APP-compliant (i.e. under APP 8.1), the Australian entity bears legal responsibility for any breaches of the APPs by the recipient.²³

12.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

No. The entity itself must assess whether or not the foreign recipient will comply with the APPs or is subject to a similar privacy regime and, if necessary, seek the individual’s consent only.

12.4 Do transfers of personal data to other jurisdictions require a transfer impact assessment? If conducting a transfer impact assessment is only mandatory in some circumstances, please identify those circumstances.

A transfer impact assessment under the GDPR is only mandatory when an entity transfers personal data from the EU or the UK to certain non-European countries like Australia. The goal of the transfer impact assessment is to conduct a risk assessment that aims to mitigate the risks associated with the transfer of personal data.

The organisation exporting personal data outside of the EU needs to carry out this assessment, to ascertain that individuals’ rights are protected and maintained in the same way they must be protected under the GDPR.²⁴

12.5 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?

In Australia, there is no official guidance from the OAIC on the *Schrems II* decision, which may help Australian organisations’ ability to show GDPR equivalence where Standard Contract Clauses (‘SCCs’) are used. The landmark *Schrems II* decision addressed the reliance of data controllers and processors on

the EU–US Privacy Shield Framework and considered the use of SCCs to demonstrate GDPR compliance.

‘The CJEU, while not invalidating SCCs, imposed additional requirements for their use. The CJEU found that SCCs won’t always be enough to ensure personal data transferred externally from the EU is adequately protected and therefore compliant with the GDPR.’²⁵ ‘Whether there is adequate protection requires a case-by-case assessment. The CJEU did not provide a full assessment framework, which has led to some uncertainty.’²⁶

Australian organisations transferring data from the EU now must promptly analyse their data flows, as doing so on a case-by-case basis is essential for compliance despite the potential burden it poses.²⁷

12.6 What guidance (if any) has/have the data protection authority(ies) issued in relation to the use of standard contractual/model clauses as a mechanism for international data transfers?

There has been no official guidance released by the OAIC in the use of standard contractual models/clauses as a mechanism for international data transfers.

13 Whistle-blower Hotlines

13.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

Protections of corporate whistleblowers are provided for in the *Corporations Act 2001* (‘**Corporations Act**’). This relates to the reporting of breaches of the Corporations Act or the *Australian Securities and Investments Commission Act 2001* (Cth).

From 1 July 2019, the whistleblower protections in Part 9.4AAA of the Corporations Act were expanded to provide greater protections for whistleblowers who report misconduct about companies and company officers. The reforms to the regime were contained in the *Treasury Laws Amendment (Enhancing Whistleblower Protections) Act 2019*, which received Royal Assent on 12 March 2019.²⁸

The changes to the Corporations Act broaden the scope of protected disclosures, encompassing a wider range of conduct related to ‘misconduct’ or an ‘improper state of affairs’, with definitions expanded. Previously, protected disclosures were limited to contraventions of the Corporations legislation. Under the amendments, whistleblowers can make anonymous disclosures without the requirement of ‘good faith’, although reasonable grounds for concern are necessary.²⁹

Whistleblowers are protected from any litigation (civil or criminal), employment termination or victimisation as a result of their actions. To qualify for these protections, a person must:

- be an officer, employee or contractor of the company in question;
- disclose to a company auditor (or member of the audit team), officer or senior manager, a person authorised to receive whistleblower disclosure or the Australian Securities and Investments Commission; or
- have reasonable grounds to suspect that the information being disclosed about the company or organisation concerns misconduct, or an improper state of affairs or circumstances.

13.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous whistleblowers are afforded the same protections under the Corporations Act as discussed in the previous sections.

Australian businesses address the issues of anonymity by enshrining the rights of anonymous whistleblowers within their corporate governance framework and whistleblower policies that must comply with S.137AI (5)(c) of the Corporations Act, which ensures whistleblower policies must have 'information about how the company will support (all) whistleblowers and protect them from detriment'.³⁰

14 CCTV

14.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

In Australia, the regulations surrounding the use of CCTV cameras vary depending on the jurisdiction.

Federal jurisdiction

Generally, the *Surveillance Devices Act 2004* (Cth) governs the practices for organisations and agencies on the usage of surveillance devices such as CCTV.³¹ The OAIC has stated that:

'If the Privacy Act covers the organisation or agency, then any personal information they collect through a surveillance device must comply with the Australian Privacy Principles. The Privacy Act covers Australian Government agencies and organisations with an annual turnover of more than \$3 million, and some other organisations. Such an organisation or agency must:

- *tell you that your image may be captured before you're recorded; and*
- *make sure recorded personal information is secure and destroyed or de-identified when it is no longer needed.'*³²

The Privacy Act does not cover security cameras operated by an individual acting in a private capacity, but state or territory laws may apply to that person.³³

State and territories jurisdiction

The governance for surveillance devices will differ between states and territories. For instance, a comparison will be drawn between NSW and QLD:

- In NSW, the use of CCTV is regulated under the *Surveillance Devices Act 2007* (NSW).³⁴ The legislation has strict requirements that should be consulted with the relevant authorities for compliance. There is a voluntary register that is maintained by NSW police, if private residents wish to register their private CCTV systems.³⁵
- In QLD, entities using CCTV are required to take 'reasonable steps' to make individuals aware of the purpose and authority for camera surveillance, although specific requirements may vary.³⁶

The examples cited above broadly explain how corporate bodies would be governed.

The OIAC has recommended for individuals, regarding compliance with state or territory laws on surveillance devices, it would be appropriate to contact the relevant state or territory Attorney-General department.³⁷

14.2 Are there limits on the purposes for which CCTV data may be used?

Similarly to above, the limitations will vary between jurisdictions.

15 Employee Monitoring

15.1 What types of employee monitoring are permitted (if any), and in what circumstances?

There is no federal legislation that governs what types of employee monitoring are permissible and under what circumstances it is permitted, this is relegated to the states and territories to govern on. Examples below will consider NSW and VIC.

In NSW, under the *Workplace Surveillance Act 2005* Part 2,³⁸ the notice requirements that employers must adhere for compliance are listed. Notably, employees are given a minimum of 14 days' notice prior to surveillance being conducted. The notice will list the circumstances for surveillance being conducted.

In VIC, under the *Surveillance Devices Act 1999* Part 2A,³⁹ the surveillance of employees in certain places and circumstances is prohibited.

15.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

As outlined above, in NSW employees must be given at least 14 days' notice or notice prior to their commencing work.⁴⁰ This must include various details about the nature and extent of the monitoring. For VIC, there is no specific timeframe listed for notice.

15.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

There is no requirement under Australian privacy law for employee representatives or trade unions to be notified or consulted regarding employee monitoring.

15.4 Are employers entitled to process information on an employee's attendance in office (e.g., to monitor compliance with any internal return-to-office policies)?

Employers may be entitled to process information on an employee's attendance if it is required as part of the internal return-to-office policy that forms the employment relationship, in which the employee's records exemption may apply and that employers will not need to comply with the Privacy Act's requirements as stated by the OAIC.⁴¹

The OAIC does warn that this exemption does not apply to practices that are outside the scope of the employment relationship.⁴²

16 Data Security and Data Breach

16.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Generally, APP entities are responsible for ensuring that data

is kept secure. The definition for APP entities is defined under section 6(1) of the Privacy Act. An APP entity is defined as an agency or organisation, in which 'organisation' can be an individual, body corporate, partnership, unincorporated association or trust.⁴³

The OAIC has published guidance on the security of personal information under APP 11. The OAIC has stated that: 'An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure.'⁴⁴

16.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

The OAIC has a Notifiable Data Breach ('NDB') scheme, where a *Privacy Act*-covered organisation or agency is required to report to the OAIC and relevant individual that an eligible data breach has occurred.⁴⁵

The OAIC has defined 'eligible data breach' as:

- unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an organisation or agency holds;
- that is likely to result in serious harm to one or more individuals; and
- the organisation or agency has not been able to prevent the likely risk of serious harm with remedial action.⁴⁶

The notification to the individual from an organisation or agency should list recommendations on what the next steps in response to the data breach should look like, ideally using the OAIC's NDB form.⁴⁷

16.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

The OAIC has published guidance on responding to data breaches; there are four steps, which are contain, assess, notify and review. There is an emphasis that data breaches should be considered on a case-by-case basis and that the notify section of the four-step response details how individuals affected by the breach should be notified.⁴⁸

The OAIC has stated that there are obligations for entities under the NDB scheme to assess a suspected breach under section 26WH(1) of the Privacy Act,⁴⁹ in which the entity must take all reasonable steps to complete the assessment within 30 days from when the entity became aware of the eligible data breach under section 26WH(2).⁵⁰

Entities will have three options for notifying individuals at risk of serious harm, depending on what is 'practicable' for the entity under section 26WH(2). The options are 'notify all individuals',⁵¹ 'notify only those individuals at risk of serious harm'⁵² and 'publish notification'. The OAIC has published guidance on what is expected to be included in an eligible data breach statement.⁵³

16.4 What are the maximum penalties for personal data security breaches?

In light of recent data breach scandals, the Australian Government passed the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022.⁵⁴

The current penalties have been laid out by the OAIC as of March 2024:⁵⁵

- 'Under s 13G of the Privacy Act, the maximum penalty for serious or repeated interferences with privacy are:
- For a body corporate, the greater of either:
 - \$50 million;
 - the value of any benefit the relevant court has determined that the body corporate, or any body corporate related to it, has obtained directly or indirectly that is reasonably attributable to the contravention, multiplied by three; or
 - if the court cannot determine the value of that benefit, 30% of the annual turnover of the body corporate during the 12-month period ending at the end of the month in which the contravention happened or began.
 - For a person other than a body corporate, the maximum penalty amount is \$2.5 million.'

17 Enforcement and Sanctions

17.1 Describe the enforcement powers of the data protection authority(ies).

(a) Investigative powers:

The Commissioner of the OAIC can initiate an investigation under section 40 of the Privacy Act.⁵⁶ Section 40(2) of the Privacy Act enables the Commissioner to initiate an investigation where:

- a. an act or practice may be an interference with the privacy of an individual or a breach of APP 1; and
- b. the Commissioner thinks it is desirable to do so.⁵⁷

The OAIC stated that: 'Prior to commencing an investigation, the Commissioner may conduct preliminary inquiries under section 42(2) of the Privacy Act, to determine whether to commence a Commissioner Initiated Investigation ('CII'). Once a CII has been commenced, the OAIC will conduct its investigation in accordance with Part V of the Privacy Act.'⁵⁸

If the OAIC does in its discretion decide to initial a CII, there are four next steps that will occur:

1. Notification to the respondent: the OAIC will notify the respondent in writing about its decision to commence a CII and about the initial scope of the investigation.
2. Information gathering: the OAIC will seek the co-operation of the respondent in the provision of necessary information.
3. Decision making: as part of the preliminary review, if the correspondent fails to meet the requirements of the Privacy Act or the requirements of the privacy safeguards or CDR rules, the Commissioner may make the following regulatory actions:
 - i. exercise a discretionary power under section 41 of the Privacy Act to discontinue an investigation;
 - ii. seek an enforceable undertaking under section 33E of the Privacy Act and section 56EW of the Competition and Consumer Act;

- iii. make a determination under section 52(1A) of the Privacy Act;
 - iv. seek an injunction under section 80W of the Privacy Act;
 - v. apply for a civil penalty order under section 80U of the Privacy Act and section 56EU of the Competition and Consumer Act; or
 - vi. report to the Minister about a CII under section 30 of the Privacy Act.
4. Conclusion and publication: the OAIC will place a notice on its website advising the public that the investigation of said matter has concluded.⁵⁹

(b) Corrective powers:

The OAIC has advised that APP 13 will 'require an APP entity to take reasonable steps to correct information to ensure that, having regard to the purpose for which it is held, it is accurate and up-to-date, complete, relevant and not misleading'.⁶⁰

The OAIC has an exhaustive explanation on the minimal procedural requirements that is expected in the correction of information.⁶¹

(c) Authorisation and advisory powers:

Authorisation: The OAIC has published guidance on authorisation, particularly with regard to consumer authorisation,⁶² in which a data holder must ask for a consumer's authorisation before disclosing their CDR to an accredited data recipient. There are minimum requirements that data holders must meet for the authorisation notice.

Advisory: The OAIC has powers under the Privacy Act and other legislative instruments to make and approve legally binding rules and guidelines as part of its advisory powers.⁶³ These guidelines help guide other agencies and APP entities who can use the guides to remain compliant with data laws and regulations.

(d) Imposition of administrative fines for infringements of specified legal provisions:

The OAIC can issue infringement notice under section 80UB of the Privacy Act with Part 5 of the Regulatory Powers Act, where the Commissioner is of the belief that a contravention under section 66(1) of the Privacy Act has occurred because the individual has failed to give information, answer a question, or produce a document or record when required to do so under the Privacy Act.⁶⁴

The infringement notice must be issued within 12 months of the alleged contravention, the expected penalty will be 12 units for a person and 60 for bodies corporate.

The OAIC has stated that any recipient of an infringement notice is permitted to seek a withdrawal of the infringement notice through written representations to the Commissioner; the OAIC has published further guidance on what is expected of the written representations.

(e) Non-compliance with a data protection authority:

In cases of non-compliance, particularly for serious or repeated offences, the Commissioner under section 80W may apply to the Federal Court for an order against an entity that is alleged to have contravened a civil penalty provision of the Privacy Act at the Commissioner's discretion.⁶⁵

The OAIC has highlighted what 'civil penalty provisions' below:

- 'a serious or repeated interference with privacy (s 13G) with maximum penalties including \$2.5 million for a person other than a body corporate, and for a body corporate, an amount not exceeding the greater of:

- \$50 million;
- three times the value of the benefit obtained directly or indirectly by the body corporate and any related bodies corporate, that is reasonably attributable to the conduct constituting the contravention; or
- if the court cannot determine the value of the benefit, 30% of the body corporate's adjusted turnover during the breach turnover period for the contravention; and
- various civil penalty provisions set out in Part IIIA – credit reporting, with penalties of either 500, 1,000 or 2,000 penalty units.'

17.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The OAIC has powers to apply for an injunction under section 80W of the Privacy Act through application to the Federal Court to restraint a person from engaging in a particular conduct and if the Court's opinion is that it is 'desirable' to do so.⁶⁶

With regard to bans on a particular processing activity, the courts must be satisfied that 'a person has engaged, is engaging in, or is proposing to engage in conduct in contravention of either the Privacy Act, the MHR Act or a privacy safeguard set out in Part IVD of the Competition and Consumer Act'.⁶⁷

17.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

An example of the OAIC's investigative powers can be seen in the case of *Cardiac Dynamics (Privacy)* [2023] AICmr 96 (24 October 2023), the OAIC had opened an investigation into the respondent's compliance with rules within the *MRH Rules 2016*.⁶⁸

The Commissioner found that the respondents had challenges in producing documents and were not utilising the MHR system despite being registered to do so. The respondent did not have a written policy that complied with rule 42 of the MHR, which required health providers to have a written policy on the use of the MHR system.

The Commissioner made a determination under section 52(1A)(a) and (b) that the respondent must take specific steps outlined to ensure the act or practice is not repeated.

17.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

The Commissioner under section 33A of the Privacy Act may share information with international bodies, which can comprise an authority of the government of a foreign country that functions to protect the privacy of individuals, similarly to the foreign equivalents of the OAIC.⁶⁹

There are safeguard limitations in section 33A that ensures the exercise of this information sharing power is 'reasonable, necessary and proportionate'.⁷⁰

In terms of enforcement, the OAIC is part of the Global Privacy Enforcement Network, which helps cross-border enforcement.

18 E-discovery/Disclosure to Foreign Law Enforcement Agencies

18.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Guidance on cross-border disclosure of information can be found in the OAIC's guide on APP 8, which details what reasonable steps an APP entity must take prior to the disclosure of personal information to an overseas recipient, in that the entity would not breach any APPs.⁷¹

The OAIC has allowed for the disclosure of personal information to an overseas recipient as required or authorised under an international agreement related to information sharing under APP8.2(e). However, the OAIC has stated that there are requirements that the agreement must make specific arrangements for disclosure of information such as identifying agency, recipient, categories of personal information that may be disclosed and circumstances where information will be disclosed.⁷²

Australia is also party to a number of international agreements that relate to the sharing of data across national borders. Although concerning the actions of public bodies, not businesses, they are of central relevance to the sharing of Australian information with foreign law enforcement. These instruments include the following examples:

- a. The 'Five Eyes' is an intelligence pact between Australia, the United States, the United Kingdom, New Zealand and Canada, all parties to the *UKUSA Agreement*. Part of this arrangement is 'critical information sharing' between the nations that relates to issues of law enforcement, border protection and criminal justice. These partners also share information concerning financial sector intelligence.⁷³
- b. Australia is party to over 25 bilateral mutual legal assistance treaties with foreign nations. All these treaties contain provisions explicitly contemplating the exchange of information between governments in relation to criminal matters.⁷⁴
- c. Australia is a party to the multilateral 2001 *Budapest Convention on Cybercrime*. Over 70 nations are parties to this treaty. The Budapest Convention covers a range of issues related to international cyber-crime, including requests to/from foreign states for the seizure, collection and interception of computer data. Article 26 specifically contemplates the spontaneous sharing of information between nations, without any prior request, that may be used in the investigation or prosecution of cyber-crime offences.⁷⁵
- d. Australia is also party to a number of Taxation Information Exchange Agreements ('TIEAs') with states outside the Organisation for Economic Cooperation and Development. TIEAs facilitate the exchange of information between countries concerning taxation matters and are aimed at combatting international tax avoidance.⁷⁶

18.2 What guidance has/have the data protection authority(ies) issued on disclosure of personal data to foreign law enforcement or governmental bodies?

On disclosure of personal data to foreign law enforcement and governmental bodies, the OAIC has broadly issued guidance to APP entities on the reasonable steps to ensure an overseas recipient does not breach any APPs.⁷⁷

The OAIC has stated that the 'requirement in APP 8.1 to ensure that an overseas recipient does not breach the APPs is qualified by a reasonable steps test'. It is generally expected that an APP entity will enter into an enforceable contractual arrangement with an overseas recipient that will enforce and require the recipient to govern the personal information in accordance with the APPs.⁷⁸

19 Artificial Intelligence

19.1 Are there any limitations on automated decision-making involving the processing of personal data using artificial intelligence?

There are some provisions in Australian legislation, while not specifically geared towards artificial intelligence ('AI'), that capture the processing of data.⁷⁹

The Privacy Act is the primary legislation governing the handling of personal information in Australia. While the Act does not specifically regulate automated decision-making, several provisions – particularly within the APPs – are relevant to the use of personal data in such systems.

APP 1, which concerns the open and transparent management of personal information, requires organisations to be clear and upfront about how they collect, use and disclose personal data, including where automated systems are involved. This includes maintaining a clearly expressed and up-to-date privacy policy that outlines the use of automation where relevant.

APP 5 deals with the notification of the collection of personal information. It requires entities to inform individuals at or before the time of collection (or as soon as practicable thereafter) about the purpose for which their information is being collected, including if it will be used in automated decision-making processes.

APP 6 relates to the use and disclosure of personal information. It limits organisations to using or disclosing personal information only for the primary purpose for which it was collected, unless an exception applies. This principle ensures that any use of personal data for automated decision-making must align with the original purpose of collection or fall within a permitted exception.

Although the Privacy Act does not expressly regulate algorithmic or AI-based decisions, these principles impose obligations that indirectly constrain how personal information can be used in such contexts. As a result, entities deploying AI systems that process personal data must ensure compliance with the APPs to mitigate legal and regulatory risk.

19.2 What guidance (if any) has/have the data protection authority(ies) issued in relation to the processing of personal data in connection with artificial intelligence?

In Australia, while there is no AI-specific legislation, the OAIC has provided important guidance on the use of AI, particularly in relation to the handling of personal information under the Privacy Act and the APPs.⁸⁰

The OAIC's guidance emphasises that organisations using AI systems should adopt a privacy-by-design approach, ensuring that personal information is handled lawfully, transparently and fairly throughout the data lifecycle. Key issues highlighted include minimising data collection, securing personal information, and ensuring transparency and explainability when

AI is used to make decisions that may significantly impact individuals. While the Privacy Act does not currently contain a specific right to human review or explanation of automated decisions (unlike the EU GDPR), the OAIC encourages entities to implement accountability mechanisms and human oversight, especially when decisions made by AI affect access to services or rights.⁸¹

The OAIC has released two guides to clarify how Australia's privacy laws apply to AI.⁸²

- **Guidance on Privacy and the Use of Commercially Available AI Products:** This guide assists organisations in complying with privacy obligations when using AI products like chatbots and content-generation tools. It emphasises conducting due diligence, embedding human oversight and regularly reviewing AI products to ensure they remain fit for purpose and compliant with privacy laws.⁸³
- **Guidance on Privacy and Developing and Training Generative AI Models:** Targeting developers, this guide highlights the need to assess whether training data contains personal or sensitive information and ensures that its use complies with privacy obligations.⁸⁴

In collaboration with the Australian Cyber Security Centre, the OAIC also released a joint statement on responsible AI use (2023), which reinforces the importance of robust security and de-identification practices when using personal data in AI training and inference processes. This joint guidance reflects increasing regulatory interest in safeguarding against misuse of personal data in AI development.

The OAIC also contributed to the development of the Australian Government's AI Ethics Principles, released in 2019 by the Department of Industry, Science and Resources. These eight voluntary principles include: human-centred values; privacy protection; fairness; transparency; contestability; and accountability. While non-binding, these principles are widely regarded as best practice for ethical AI use, particularly in government and regulated sectors.⁸⁵

20 Trends and Developments

20.1 In your opinion, what enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.

The trending topic concerning enforcement over the previous 12 months and prior has primarily been reform to the privacy act to bolster enforcement and investigative powers.⁸⁶

On 29 November 2024, the Privacy and Other Legislation Amendment Bill 2024 passed both Houses of the Australian Parliament, representing the first phase of long-anticipated reforms to modernise Australia's privacy framework in the digital era.⁸⁷ The Bill introduces significant enhancements to the enforcement and investigative powers of the OAIC, as well as a new tiered penalty regime. These changes are designed to strengthen the OAIC's ability to hold entities accountable for mismanagement of personal information and will come into force once the Bill receives Royal Assent.

Under the current Privacy Act, the OAIC already possesses the authority to investigate privacy breaches and initiate civil penalty proceedings. However, the frequency and scale of enforcement have remained limited, particularly in response to widespread data breaches affecting Australians in recent years. In February 2023, the Attorney-General released the Privacy Act Review Report, which proposed a suite of reforms aimed at expanding the OAIC's enforcement toolkit. These

included the introduction of a tiered penalty structure, enhancement of investigatory powers to cover civil penalty provisions, and authority for the Commissioner to conduct public inquiries.⁸⁸ The report also explored the potential for industry funding models to better resource the OAIC.

The Government's response to the report, published in September 2023, endorsed the introduction of tiered civil penalties and greater enforcement powers, while also supporting further work to ensure adequate resourcing for the OAIC, including the possibility of a contingency litigation fund.⁸⁹ The 2024 Amendment Bill sets out how these reforms will be implemented, following stakeholder consultation and impact analysis.

Substantively, the Bill revises the penalty framework by distinguishing between serious and non-serious interferences with privacy and introduces new provisions specifically targeting breaches of defined obligations under the APPs and non-compliant data breach notifications. It empowers the OAIC with revised investigation and monitoring powers and enables the Commissioner to conduct public inquiries at the direction or approval of the Minister. Additionally, federal courts are granted expanded authority to issue orders beyond pecuniary penalties in civil proceedings.

The Bill also lowers the threshold for civil penalties by amending the Privacy Act to remove the "repeated" requirement, such that serious interferences with privacy alone can now attract maximum penalties. It further clarifies the criteria for determining whether an interference is serious, including considerations such as the sensitivity of the information involved, the scale of affected individuals, the vulnerability of those individuals, and whether the organisation failed to implement adequate privacy systems. Importantly, the reforms introduce penalties for less serious privacy interferences and allow for enforcement through infringement notices or compliance notices. Compliance notices provide regulated entities with actionable steps to meet their privacy obligations and, if complied with, can shield them from civil penalties.

Together, these changes significantly enhance the OAIC's ability to respond to privacy breaches with proportional enforcement and reflect the government's broader commitment to strengthening data protection in Australia.

20.2 In your opinion, what "hot topics" are currently a focus for the data protection regulator?

The OAIC's Corporate Plan for 2024–25 outlines the agency's strategic priorities and key activities aimed at promoting and upholding privacy and information access rights in Australia.⁹⁰

In 2024, the OAIC underwent significant leadership changes, including the appointment of three commissioners: the Australian Information Commissioner; a Privacy Commissioner; and a Freedom of Information ('FOI') Commissioner. This restructuring is intended to bolster the OAIC's capacity to address the increasing complexity and volume of privacy and information access matters.

The Corporate Plan emphasises several key areas, as outlined below.⁹¹

In 2024–25, the OAIC's key activities will focus on influencing and upholding privacy and information access rights frameworks, advancing online privacy protections, encouraging proactive release of government information and taking a contemporary, harms-based approach to regulation.

Firstly, in terms of privacy regulation, the OAIC will oversee privacy laws such as the Privacy Act, focusing on complaints handling, investigations and assessments. It will continue

to monitor the privacy aspects of initiatives like the CDR, Digital ID and the My Health Record system. A priority will be ensuring that privacy protections are implemented effectively as the Digital ID system expands. Additionally, the OAIC will manage the NDB scheme, ensuring entities comply with notification requirements and guiding them on breach prevention and remediation. It will also continue regulatory actions related to high-profile data breaches, including cases involving Medibank, Optus and Latitude.

On the front of information access, the OAIC will regulate access to government-held information under the FOI Act. This includes conducting independent merit reviews of FOI decisions, investigating agency actions and promoting timely release of government information. A key focus will be finalising outstanding reviews from 2020 and 2021, and improving agencies' practices to ensure transparency and accountability. The OAIC will continue to advocate for proactive information release and will engage with government agencies to promote best practices in FOI.

Regarding online privacy protections, the OAIC will lead efforts to address the risks posed by new technologies like AI and online platforms. It will influence policy and legislation, including privacy law reforms and cyber security strategies, to protect privacy in the digital economy. The OAIC will also focus on privacy risks associated with AI, ensuring that new technologies align with community expectations and regulatory requirements. Additionally, the OAIC will continue to enforce its civil penalty proceedings against Meta Platforms, Inc., addressing the harms stemming from the Cambridge Analytica scandal.

Finally, the OAIC will take a contemporary, harms-based approach to its regulatory role. This includes adopting a risk-based strategy, focusing on high-risk areas where regulatory action is most needed to prevent harm to individuals and communities. The OAIC will use data-driven methods to assess risk and develop regulatory approaches that are fair, transparent and proportionate. It will also continue its efforts to foster a strong regulatory culture internally, building its workforce's capacity to effectively address emerging challenges, particularly in the context of new digital technologies and evolving privacy concerns.

Endnotes

- 1 'Law in Australia' DLA Piper (<https://www.dlapiperdataprotection.com/index.html?t=law&c=AU>) (last modified 31 December 2023) (accessed 30 March 2024).
- 2 *Ibid.*
- 3 'Data Protection Laws of the World' DLA Piper (<https://www.dlapiperdataprotection.com/index.html?t=data-protection-officers&c=AU>) (last modified 31 December 2023) (accessed 28 March 2024).
- 4 'Australia – Data Protection Overview' Alec Christie Clyde and Co (<https://www.dataguidance.com/notes/australia-data-protection-overview>) (October 2023) (accessed 28 March 2024).
- 5 Attorney-General's Department (Australia), *Privacy Act Review Final Report* (2022) (https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf), p44.
- 6 Office of the Australian Information Commissioner, *Privacy Officer Toolkit* (<https://education.oaic.gov.au/privacy-officer-toolkit/#section-12>) (accessed 29 March 2024).
- 7 Office of the Australian Information Commissioner, *Privacy Officer Toolkit* (<https://education.oaic.gov.au/privacy-officer-toolkit/#section-12>) (accessed 29 March 2024).
- 8 Office of the Victorian Information Commissioner, 'The Role of the Privacy Officer' (<https://ovic.vic.gov.au/privacy/resources-for-organisations/privacy-officer-toolkit/the-role-of-the-privacy-officer>) (accessed 29 March 2024).
- 9 Office of the Australian Information Commissioner, *Privacy Officer Toolkit* (<https://education.oaic.gov.au/privacy-officer-toolkit/#section-1>) (accessed 29 March 2024).
- 10 Office of the Australian Information Commissioner, *Australian Entities and the European Union General Data Protection Regulation* (<https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/more-guidance/australian-entities-and-the-european-union-general-data-protection-regulation>) (accessed 29 March 2024).
- 11 *Privacy Act 1988* (Cth) sch 1, APP 7.1 (<https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-7-app-7-direct-marketing>).
- 12 *Privacy Act 1988* (Cth) sch 1, APP 7.2 (<https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-7-app-7-direct-marketing>).
- 13 Office of the Australian Information Commissioner, *Advertising, Marketing and Spam*, (Webpage, Office of the Australian Information Commissioner, 2024) (<https://www.oaic.gov.au/privacy/your-privacy-rights/more-privacy-rights/advertising-marketing-and-spam>) (accessed 29 March 2024).
- 14 *Spam Act 2003*, section 7.
- 15 Office of the Australian Information Commissioner, *Chapter 3: APP 3 Collection of solicited personal information* (<https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-3-app-3-collection-of-solicited-personal-information>) (accessed 29 March 2023).
- 16 Katherine Kemp, 'Australia's forgotten Privacy Principle: Why Common 'Enrichment' of Customer Data for profiling and targeting is Unlawful', (2022) *University of New South Wales* (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4224653).
- 17 Office of the Australian Information Commissioner, *Chapter 3: APP 3 Collection of solicited personal information* (<https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-3-app-3-collection-of-solicited-personal-information>) (accessed 29 March 2023).
- 18 *Ibid.*, 3.65.
- 19 *Ibid.*, 3.68.
- 20 *Do Not Call Registry Act 2006*, section 25.
- 21 Office of the Australian Information Commissioner, *Targeted Online Marketing*, (<https://www.oaic.gov.au/privacy/your-privacy-rights/social-media-and-online-privacy/targeted-online-marketing>) (accessed 29 March 2024).
- 22 Melissa Fai, Andrew Hii and Claire Harris, 'Privacy Act Review Report: Highlights and Hot takes', (16 February 2023) *Gilbert and Tobin*, (<https://www.gtlaw.com.au/knowledge/privacy-act-review-report-highlights-hot-takes>) (accessed 29 March 2023).
- 23 Office of the Australian Information Commissioner, *Part 8: Overseas data flows* (<https://www.oaic.gov.au/engage-with-us/submissions/privacy-act-review-issues-paper-submission/part-8-overseas-data-flows>) (accessed 29 March 2023).
- 24 Lillian Zhang, 'Transfer Impact Assessments (TIAs)' (29 August 2023) *Harper James Solicitors* (<https://harperjames.co.uk/article/transfer-impact-assessments-tias/#section-1>) (accessed 29 March 2023).
- 25 Dan Pearce and Louise Almedia, 'Schrems II: What is the Australian impact of the GDPR decision?' (31 March 2021) *Holding Redlich* (https://www.holdingredlich.com/schrems-ii-what-is-the-australian-impact-of-the-gdpr-decision?utm_source=mondaq&utm_medium=syndication&utm_term=privacy&utm_content=articleoriginal&utm_campaign=article) (accessed 29 March 2023).

- 26 *Ibid.*
- 27 Paul Kallenbach, Zita Megyeri and Darcy O'Brien, 'Schrems II: What the end of the EU–US Privacy Shield means in Australia' (12 November 2020) *MinterEllison* (<https://www.minterellison.com/articles/what-the-end-of-the-eu-us-privacy-shield-means-in-australia>) (accessed 29 March 2023).
- 28 Australian Securities Investigation Commission, *Protection for Corporate Sector Whistleblowers* (<https://asic.gov.au/about-asic/asic-investigations-and-enforcement/whistleblowing/protectations-for-corporate-sector-whistleblowers>) (accessed 29 March 2023).
- 29 Abigail McGregor, 'A new era for Whistleblowers in Australia', (January 2023), (<https://www.nortonrosefulbright.com/en/knowledge/publications/63b0f230/update-on-new-whistleblower-protection-laws-in-australia>) (accessed 29 March 2023).
- 30 *Corporations Act 2001*, section 137AI (5)(c).
- 31 *Surveillance Devices Act 2004* (Cth).
- 32 Office of the Australian Information Commissioner, 'Security Cameras' (Government website) (<https://www.oaic.gov.au/privacy/your-privacy-rights/surveillance-and-monitoring/security-cameras>).
- 33 *Ibid.*
- 34 *Surveillance Devices Act 2007* (NSW).
- 35 NSW Police Force, CCTV Register (PDF Brochure) (https://www.police.nsw.gov.au/__data/assets/pdf_file/0011/105113/nsw_cctv_brochure.pdf).
- 36 Office of the information Commissioner Queensland, Camera Surveillance and Privacy (Government Website) (<https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/collection/camera-surveillance-and-privacy>).
- 37 Office of the Australian Information Commissioner, 'Security Cameras' (Government website) (<https://www.oaic.gov.au/privacy/your-privacy-rights/surveillance-and-monitoring/security-cameras>).
- 38 *Workplace Surveillance Act 2005* (NSW) Part 2.
- 39 *Surveillance Devices Act 1999* (VIC) Part 2A.
- 40 *Workplace Surveillance Act 2005* (NSW) Part 2 sections 10–13.
- 41 Office of the Australian Information Commissioner, 'Employee records exemption' (Government website) (<https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/organisations/employee-records-exemption>).
- 42 *Ibid.*
- 43 Office of the Australian Information Commissioner, 'Chapter 11: APP 11 Security of personal information'. (Government website) (<https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-11-app-11-security-of-personal-information>).
- 44 *Ibid.*
- 45 Office of the Australian Information Commissioner, 'Report a data breach' (Government website) (<https://www.oaic.gov.au/privacy/notifiable-data-breaches/report-a-data-breach>).
- 46 *Ibid.*
- 47 Office of the Australian Information Commissioner, 'About the Notifiable Data Breaches scheme' (Government website) (<https://www.oaic.gov.au/privacy/notifiable-data-breaches/about-the-notifiable-data-breaches-scheme>).
- 48 Office of the Australian Information Commissioner, 'Part 3: Responding to data breaches – four key steps' (Government website) (<https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/preventing-preparing-for-and-responding-to-data-breaches/data-breach-preparation-and-response/part-3-responding-to-data-breaches-four-key-steps>).
- 49 *Privacy Act 1988* (Cth) section 26WH(1).
- 50 *Privacy Act 1988* (Cth) section 26WH(2).
- 51 *Privacy Act 1988* (Cth) section 26WL(2)(a).
- 52 *Privacy Act 1988* (Cth) section 26WL(2)(b).
- 53 Office of the Australian Information Commissioner, 'What to include in an eligible data breach statement', (Government website) (<https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/preventing-preparing-for-and-responding-to-data-breaches/data-breach-preparation-and-response/part-4-notifiable-data-breach-ndb-scheme#assessing-a-suspected-data-breach>).
- 54 Attorney-General (Cth), 'Parliament approves Government's privacy penalty bill' (Media release, 28 November 2022).
- 55 Office of the Australian Information Commissioner, 'Civil Penalties – serious or repeated interferences with privacy and other penalty provisions' (Government website) (<https://www.oaic.gov.au/about-the-OAIC/our-regulatory-approach/guide-to-privacy-regulatory-action/chapter-7-privacy-assessments>).
- 56 *Privacy Act 1988* (Cth) section 40.
- 57 *Privacy Act 1988* (Cth) section 40(2).
- 58 Office of the Australian Information Commissioner, 'Chapter 2: Commissioner initiated investigations and referrals' (Government website) (<https://www.oaic.gov.au/about-the-OAIC/our-regulatory-approach/guide-to-privacy-regulatory-action/chapter-2-commissioner-initiated-investigations-and-referrals>).
- 59 *Ibid.*
- 60 Office of the Australian Information Commissioner, 'Chapter 13: APP 13 Correction of personal information' (Government website) (<https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-13-app-13-correction-of-personal-information>).
- 61 *Ibid.*
- 62 Office of the Australian Information Commissioner, 'Consumer consent, authorisation and dashboards' (Government website) (<https://www.oaic.gov.au/consumer-data-right/consumer-data-right-guidance-for-business/privacy-obligations/consumer-consent-authorisation-and-dashboards>).
- 63 Office of the Australian Information Commissioner, 'Rules and guidelines' (Government website) (<https://www.oaic.gov.au/privacy/privacy-legislation/the-privacy-act/rules-and-guidelines>).
- 64 Office of the Australian Information Commissioner, 'Chapter 8: Infringement notices' (Government website) (<https://www.oaic.gov.au/about-the-OAIC/our-regulatory-approach/guide-to-privacy-regulatory-action/chapter-8-infringement-notices>).
- 65 Office of the Australian Information Commissioner, 'Civil Penalties – serious or repeated interferences with privacy and other penalty provisions' (Government website) (<https://www.oaic.gov.au/about-the-OAIC/our-regulatory-approach/guide-to-privacy-regulatory-action/chapter-7-privacy-assessments>).
- 66 *Privacy Act 1988* (Cth) section 80W.
- 67 Office of the Australian Information Commissioner, 'Chapter 6: Injunctions' (Government website) (<https://www.oaic.gov.au/about-the-OAIC/our-regulatory-approach/guide-to-privacy-regulatory-action/chapter-6-injunctions>).
- 68 *Cardiac Dynamics (Privacy)* [2023] AICmr 96 (24 October 2023).
- 69 <https://www.oaic.gov.au/about-the-OAIC/our-regulatory-approach/guide-to-privacy-regulatory-action/chapter-3-information-sharing#information-sharing-with-other-authorities>
- 70 *Privacy Act 1988* (Cth) section 33A.

- 71 Office of the Australian Information Commissioner, 'Chapter 8: APP8 Cross-border disclosure of personal information' (Government website) (<https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information#when-does-an-app-entity-disclose-personal-information-about-an-individual-to-an-overseas-recipient>).
- 72 *Ibid.*
- 73 Australian Signals Directorate, Intelligence partnerships (Government website) (<https://www.asd.gov.au/about/history/75th-anniversary/stories/2022-03-16-intelligence-partnerships>).
- 74 Attorney General (Cth), 'Mutual assistance overview' (Government website) (<https://www.ag.gov.au/international-relations/publications/mutual-assistance-overview>).
- 75 Austlii, 'Accession by Australia to the Convention on Cybercrime' (Legal database) (<https://www.austlii.edu.au/au/other/dfat/nia/2011/9.html>).
- 76 Australian Taxation Office, 'Tax information exchange agreements – overview' (Government website) (<https://www.ato.gov.au/about-ato/international-tax-agreements/in-detail/tax-information-exchange-agreements-tiea/tax-information-exchange-agreements-overview>).
- 77 Office of the Australian Information Commissioner, 'Chapter 8: APP 8 Cross-border disclosure of personal information' (Government website) (<https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information>).
- 78 *Ibid.*
- 79 *Privacy Act 1988* (Cth) — Part IIIB.
- 80 <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/guidance-on-privacy-and-the-use-of-commercially-available-ai-products>
- 81 *Ibid.*
- 82 <https://www.mondaq.com/australia/privacy-protection/1538958/the-crossroads-of-ai-and-privacy-compliance-oaic-publishes-new-guidance>
- 83 <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/guidance-on-privacy-and-the-use-of-commercially-available-ai-products>
- 84 <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/guidance-on-privacy-and-developing-and-training-generative-ai-models>
- 85 <https://www.finance.gov.au/sites/default/files/2024-06/National-framework-for-the-assurance-of-AI-in-government.pdf>
- 86 *Privacy and Other Legislation Amendment Bill 2024*.
- 87 https://www.aph.gov.au/Parliamentary_Business/Bills_LEGislation/Bills_Search_Results/Result?bld=r7249
- 88 <https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report>
- 89 <https://www.ag.gov.au/rights-and-protections/publications/government-response-privacy-act-review-report>
- 90 Office of the Australian Information Commissioner Corporate Plan 2024–25: <https://www.oaic.gov.au/about-the-OAIC/our-corporate-information/corporate-plans/corporate-plan-2024-25>
- 91 <https://www.oaic.gov.au/about-the-OAIC/our-corporate-information/corporate-plans/corporate-plan-2024-25>



Darren Pham is a defence lawyer who is part of the white-collar investigations team, where he brings his deep experience in risk advisory, money laundering, fraud, corruption, bribery and sanctions to complex local and international investigations. Darren is experienced in advising banks, insurance companies, superannuation funds and casinos on their operational policies, governance frameworks and internal audit compliance.

Nyman Gibson Miralis

9/299 Elizabeth Street
Sydney, NSW, 2000
Australia

Tel: +61 2 9264 8884
Email: dp@ngm.com.au
LinkedIn: www.linkedin.com/in/darren-pham



Phillip Salakas is a lawyer who works in our international white-collar crime practice and primarily works on matters under investigation and prosecution by the Australian Taxation Office (ATO), the Australian Federal Police (AFP) and the New South Wales Police force. Phillip also has experience working in our international crime team, working on INTERPOL matters involving Red and Blue notices, managing various extradition requests, and assisting the partners in advising on complex matters involving the Australian Sanctions Office.

Phillip has also worked with high-net-worth clients on remediation governance projects in relation to drafting policies and procedures for compliance with international Sanctions, Anti-Bribery and Corruption, and Anti-Money Laundering and Counter-Terrorism Financing.

Nyman Gibson Miralis

9/299 Elizabeth Street
Sydney, NSW, 2000
Australia

Tel: +61 2 9264 8884
Email: psa@ngm.com.au
LinkedIn: www.linkedin.com/in/phillip-salakas



Harry Sultan is a criminal defence lawyer with a practice spanning from white-collar crime and internal investigations to serious general crime and administrative investigations.

He has represented clients under investigation by administrative bodies including the Australian Tax Office, the Serious Financial Crime Taskforce, the Australian Securities and Investments Commission and the Independent Commission against Corruption.

Harry also represents clients in serious criminal matters prosecuted by State and Commonwealth authorities at all levels of the court hierarchy. He has experience appearing in the District and Local Courts throughout New South Wales.

Nyman Gibson Miralis

9/299 Elizabeth Street
Sydney, NSW, 2000
Australia

Tel: +61 2 9264 8884
Email: hs@ngm.com.au
LinkedIn: www.linkedin.com/in/harry-sultan-98198ab5

Nyman Gibson Miralis is an international, award-winning criminal defence law firm based in Sydney, Australia. For over 55 years it has been leading the market in all aspects of general, complex and international crime, and is widely recognised for its involvement in some of Australia's most significant criminal cases.

Our international law practice focuses on white-collar and corporate crime, transnational financial crime, international sanctions, bribery and corruption, international money-laundering, cybercrime, international asset-freezing/forfeiture, extradition and mutual-assistance law.

Nyman Gibson Miralis strategically advises and appears in matters where cross-border investigations and prosecutions are being conducted in parallel jurisdictions, involving some of the largest law enforcement agencies and financial regulators worldwide.

Working with our international partners, we have advised and acted in investigations involving the British Virgin Islands, Cambodia, Canada, China, the EU, Hong Kong, Macao, Mexico, New Zealand, Russia, South Africa, South Korea, Singapore, Taiwan, the UK, the US and Vietnam.

www.ngm.com.au

ngm
NYMAN
GIBSON MIRALIS
Defence Lawyers and Advisors est. 1966

Brazil

Pinheiro Neto Advogados



Larissa
Galimberti



Luiza Fonseca
de Araujo



Cecília Alberton
Coutinho Silva

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The General Data Protection Law (Law No. 13,709) (*Lei Geral de Proteção de Dados* – known as the “LGPD”) is the principal data protection legislation in Brazil. The LGPD was enacted in August 2018 and came into force on September 18, 2020 (except for the chapter on administrative penalties provided by the LGPD, which came into force in August 1, 2021).

1.2 Is there any other general legislation that impacts data protection?

Yes. Before the enactment of the LGPD, privacy was generally protected in Brazil through the Federal Constitution, the Civil Code (Law No. 10,406/2002), the Consumer Protection Code (Law No. 8,078/1990), the Brazilian Internet Law (Law No. 12,965/2014) and Decree No. 8,771/2016, which regulates the Brazilian Internet Law. In addition, the Access to Information Law (Law No. 12,527/2011) provides regulation on the access to public information in Brazil.

Constitutional Amendment No. 115/2022 added to Article 5, LXXIX, of the Brazilian Federal Constitution the right to the protection of personal data, including in digital media, as a fundamental right, in addition to the right to privacy and the private life of individuals provided in Article 5, X, of the Brazilian Federal Constitution.

The Brazilian Civil Code also assures individuals with the right to seek judicial relief to prevent the continuous infringement of their privacy rights and the right to claim indemnification for all damages arising thereof (Articles 20 and 21).

The Consumer Protection Code provides for specific rules in connection with the creation of consumer databases (Article 43). The creation of databases with consumer records must be informed to consumers whose information will be collected, and such records cannot contain any negative information that is more than five years old. Consumers must be granted access to information collected about them and they have the right to demand any correction deemed necessary.

The Brazilian Internet Law also establishes rules that apply to application providers; for instance, the Brazilian Internet Law provides for personal data retention obligations. Application providers must store log information (access date and time associated to an IP address) for, at least, six months (Article 15).

1.3 Is there any sector-specific legislation that impacts data protection?

Yes. Specific sectors also have regulations that impact data protection, for instance, the banking, health and electoral sectors.

Banking sector

Entities regulated by the Central Bank of Brazil (“BCB”) are subject to specific law and regulation, such as the Banking Secrecy Law (Supplementary Law No. 105/2001) and the Cybersecurity Regulation (Brazilian National Monetary Council (“CMN”) Resolution No. 4,893/2021, and the Central Bank Circular No. 85/2021), among others.

According to the Banking Secrecy Law, financial entities must keep confidential “all of their credit and debit transactions, as well as the services rendered”. The specific situations in which information may be disclosed without being considered a breach of the Banking Secrecy Law are listed in Article 1, paragraph 3; for example: (i) exchange of information between financial entities or ancillary entities for credit protection; (ii) disclosures determined by law or ordered by a competent authority; and (iii) disclosures expressly authorised by the interested parties (i.e., the client).

The Cybersecurity Regulation provides rules applicable to regulated financial institutions and payment institutions, in connection with certain local requirements for storing and processing data, such as: (i) internal cybersecurity governance requirements; (ii) requirements for hiring outsourced relevant services regarding cloud computing and data processing; (iii) establishing a cybersecurity policy; and (iv) storing data outside Brazil.

The Positive Data Law (Law No. 12.414/2011), Decree No. 9,936/19 and CMN Resolution No. 4,737/19 altogether regulate the creation and management of databases containing information on the payment record of individuals or legal entities, aimed at building a positive credit history.

On May 10, 2020, the CMN and the BCB issued Joint Resolution No. 1/2020 containing the main regulation for the Brazilian Open Finance framework. Open Finance consists of the sharing of customer data and comprises payment initiation services and the forwarding of credit transaction proposals by financial institutions, payment institutions and other BCB-authorised entities through the integration of platforms and infrastructure of information systems.

One of the goals of Open Finance is to facilitate the access to information and to enhance transparency among the institutions and their customers. To that end, the institutions are required to safeguard the security and privacy of data

and services shared within the Open Finance environment, keeping the quality of data and the interoperability among participants. The sharing of customer data is possible only upon the data subject's explicit consent.

BCB Resolution No. 342/2023 amended the BCB Resolution No. 1/2020, which governs the operation of the PIX payment arrangement, to include specific obligations related to the communication of security breaches involving personal data within the PIX infrastructure even when the security incident may not result in harm or damages to the data subjects.

In addition, BCB Resolution No. 304/2023 approves the regulation that governs, within the scope of the Brazilian Payment System, the operation of settlement systems, the performance of registration and centralised deposit activities for financial assets, and the establishment of encumbrances and liens on registered or deposited financial assets and consolidates rules on the matter. Such resolution is applicable not only to regulated entities but to all financial market system operating institutions.

According to Resolution No. 304/2023, the contracting of relevant data processing, data storage and cloud computing services provided outside Brazil must comply with the following requirements: (i) the existence of an information exchange agreement between the BCB and the supervisory authorities of the countries where the services may be provided; (ii) the contracting institution must ensure that the provision of the services does not impair its regular operation nor hinder the actions of the BCB; (iii) the contracting institution must define, prior to contracting, the countries and the regions within each country where the services may be provided and where the data may be stored, processed and managed; and (iv) the contracting institution must provide for alternatives for business continuity in the event of the impossibility of maintaining or the termination of the service contract.

Additionally, Joint Resolution No. 6/2023 establishes requirements for the sharing of data and information regarding indications of fraud among financial institutions and payment institutions regulated or authorised by BCB. The primary objective of this resolution is to enhance fraud prevention procedures and controls by mandating that relevant data – such as information about individuals or institutions involved in actual or attempted fraud, descriptions of fraudulent activities, and details about accounts receiving suspicious funds – be shared through a secure electronic system among covered institutions.

Health sector

Entities in the health industry are subject to the Medical Ethics Code (Resolution CFM No. 2.217/2018), which determines that health professionals must abstain from disclosing any information they become aware of as a result of their activities, unless such disclosure is made with cause, due to a legal obligation or with the previous and explicit authorisation, in writing, of the patient.

Electoral sector

The Superior Electoral Court approved 12 resolutions on rules and guidelines for the elections (for mayor and city councils) that took place in October 2024. Resolution No. 23,732/2024 amends Resolution No. 23,610/2019, which specifically regulates electoral campaigns. According to Resolution No. 23,732/2024, all application providers, political parties and candidates must comply with the LGPD whenever processing personal data and establishing additional obligations.

1.4 What authority(ies) are responsible for data protection?

The Brazilian authority responsible for data protection is the *Autoridade Nacional de Proteção de Dados* (“ANPD”), which was created on December 28, 2018, through the Executive Order (MP) 869/2018, and confirmed by the Federal Law No. 13,853/2019, enacted on July 8, 2019.

The ANPD is a special autonomous agency, endowed with technical and decision-making autonomy, with its own assets, composed of five commissioners appointed by the President.

The ANPD exercises roles of: (i) regulation, issuing regulations, guides and technical notes on the interpretation of the LGPD; (ii) investigation and sanctioning, in cases of non-compliance with the law, through administrative proceedings; and (iii) education, with the responsibility of promoting knowledge of the LGPD and security measures, promoting standards of services and products that facilitate data control and preparing studies on national and international practices for the protection of personal data and privacy, among others.

However, in practice, we have seen other authorities in Brazil enforcing privacy rights through administrative procedures or lawsuits, such as the Department of Consumer Protection and Defense and the Public Prosecutor Office. In addition, individual and collective lawsuits have been filed due to alleged violation of data privacy.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

■ “Personal Data”

In January 2024, the ANPD published a Personal Data Protection Glossary with key definitions related to data protection, which can be accessed at: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/glossario-anpd-protecao-de-dados-pessoais-e-privacidade.pdf>. Personal data is any information related to an identified or identifiable natural person (Article 5, I, LGPD). Name, address, phone number, tax ID number, etc. are all examples of personal data related to an identified person, by which you can easily identify the natural person it refers to. However, there is no criteria under the data protection legislation to define an “identifiable natural person”. While the ANPD does not provide for such criteria, personal data related to identifiable natural persons may be understood as data that, in conjunction with other data, permits you to identify a natural person, such as geolocation or profiles.

■ “Processing”

Processing of personal data includes any activity carried out with personal data. For instance, collection, production, receipt, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, elimination, information control, modification, communication, transfer, diffusion and extraction are all examples of data processing activities (Article 5, X, LGPD).

■ “Controller”

The controller is the natural person or legal entity, governed either by public or private law, that is in charge of making decisions about the processing of personal data (Article 5, VI, LGPD).

The controller is responsible for determining the purpose of the data processing activity and for appointing the appropriate legal basis for each process, among other obligations.

■ **“Processor”**

The processor is the natural person or legal entity, governed either by public or private law, that processes personal data on behalf of the controller and following the controller’s instructions (Article 5, VII, LGPD).

The processor, along with the controller, are the processing agents (Article 5, IX, LGPD).

■ **“Data Subject”**

The data subject is the natural person to whom the personal data refers to (Article 5, V, LGPD).

■ **“Sensitive Personal Data”/“Special Categories of Personal Data”**

The LGPD also determines sensitive personal data (Article 5, II, LGPD). This subgroup of personal data includes any information regarding a natural person’s race or ethnic origin, religion, political opinion, trade union or religious, philosophical or political organisation membership, health, sex life, genetics or biometrics.

■ **“Data Breach”**

Data breach is defined in the ANPD’s Resolution No. 15/2024, which regulates the data breach notification process (“Resolution CD/ANPD No. 15/2024”). According to Resolution CD/ANPD No. 15/2024, a data breach is any confirmed adverse event related to the violation of the confidentiality, integrity, availability and authenticity properties of personal data security.

For the purpose of clarification, Resolution CD/ANPD No. 15/2024 also defines the following:

- (i) Confidentiality as a quality ensuring that personal data is not available or disclosed to unauthorised individuals, companies, systems, agencies or entities.
- (ii) Integrity as a quality ensuring that personal data has not been modified or destroyed in an unauthorised or accidental manner.
- (iii) Availability as a quality ensuring that personal data is accessible and usable, on demand, by an individual or a specific system, organisation or entity duly authorised.
- (iv) Authenticity as a quality ensuring that information has been produced, sent, modified or destroyed by a specific individual, equipment, system, organisation or entity.

■ **“Anonymised Data”**

Anonymised data refers to data related to a natural person that cannot be identified considering the use of reasonable technical means available at the time of the data processing (Article 5, III, LGPD). Anonymised data are not subject to the LGPD.

■ **“Data Protection Officer”**

The LGPD defines the Data Protection Officer (“DPO”) as a person appointed by the controller and the processor to act as a communication channel between the controller, the data subjects and the ANPD (Article 5, VIII, LGPD).

■ **“Consent”**

Consent is a demonstration of the data subjects that they agree to the processing of their personal data for a specific purpose (Article 5, XII, LGPD). Consent must be free, informed and unequivocal, otherwise the consent would be deemed null and void.

■ **“Data Protection Impact Assessment”**

Data protection impact assessment refers to the documentation drafted by the controller that contains a

description of the personal data processing activities that could result in risks to the civil liberties and to the fundamental rights, as well as measures, safeguards and mechanisms to mitigate risks (Article 5, XVII, LGPD).

■ **“Balancing Test”**

A proportionality assessment carried out by the controller whenever the controller uses the legal bases of “legitimate interest” or “prevention of fraud and security for the data subject in the processes of identification and authentication of registration in electronic systems”, based on the context and specific circumstances of the data processing, taking into account the impacts and risks to the rights and freedoms of data subjects (ANPD’s Guidelines on the lawful bases: Legitimate Interest).

■ **“Joint Controllership”**

The joint, common or convergent determination by two or more data controllers of the purposes and essential elements for carrying out the processing of personal data, through an agreement establishing their respective responsibilities for compliance with the LGPD (ANPD’s Guidelines on Processing Agents Definition and Data Protection Officer).

■ **“Serious Infraction”**

An infraction shall be considered “serious” when: (i) the hypothesis of a medium infraction is verified, and cumulatively, at least one of the following: (a) it involves processing personal data on a large scale; (b) the infringer derives or intends to derive economic advantage from the committed infraction; (c) the infraction poses a risk to the life of the data subjects; (d) the infraction involves processing sensitive data or personal data of children, adolescents or the elderly; (e) the infringer processes personal data without justification under one of the lawful bases provided for in the LGPD; (f) the infringer carries out processing with illicit or abusive discriminatory effects; or (g) the systematic adoption of irregular practices by the infringer is verified; or (ii) it constitutes obstruction to inspection activities (ANPD’s Resolution No. 4/2023 on the dosimetry and application of administrative sanctions (“Resolution CD/ANPD No. 4/2023”).

■ **“Medium Infraction”**

Infraction that significantly affects the interests and fundamental rights of data subjects, characterised in situations where the processing activity could significantly prevent or limit the exercise of rights or the use of a service, as well as cause material or moral harm to the data subjects, such as: discrimination; violation of physical integrity; right to image and reputation; financial fraud; or misuse of identity, provided it is not classified as serious (Resolution CD/ANPD No. 4/2023).

■ **“Minor Infraction”**

Infraction that does not fall within any of the hypotheses related to medium or serious violations (Resolution CD/ANPD No. 4/2023).

■ **“International Transfer”**

Transfer of personal data to a foreign country or international organisation of which the country is a member (Resolution CD/ANPD No. 19/24).

■ **“International Personal Data Collection”**

Collection of the data subject’s personal data carried out directly by the processing agent located abroad (Resolution CD/ANPD No. 19/24).

3 Territorial and Material Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

Yes. The LGPD may apply to businesses established in other jurisdictions as it provides for extraterritorial reach. The LGPD applies to any data processing activity carried out by natural person or by a public or private legal person, regardless of the country where they are established or the country where the data is hosted, provided one of the following requirements are met: (i) the data processing takes place within the Brazilian territory; (ii) the processing activity is intended to offer or supply goods or services or to process data of individuals located in the Brazilian territory; or (iii) the collection of personal data subject to processing has taken place in the Brazilian territory (Article 3, LGPD).

3.2 Do the data protection laws in your jurisdiction carve out certain processing activities from their material scope?

Yes. The LGPD is not applicable when the processing of personal data: (i) is carried out by a natural person for exclusively personal and non-economic purposes; (ii) is carried out for exclusively (a) journalistic and artistic purposes, or (b) academic purposes; (iii) is carried out for exclusive purposes of (a) public security, (b) national defence, (c) state security, or (d) investigation and repression of criminal offences; or (iv) is related to personal data originated from outside the national territory and which are not the subject of communication, shared use with Brazilian processing agents, or international transfer of data to another country other than the country of origin, provided that the country of origin provides a level of personal data protection appropriate to that provided for in the LGPD (Article 4, LGPD).

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
The transparency principle assures data subjects of clear, accurate and easily accessible information on processing activities and on the respective processing agents, with due regard for trade and industrial secrets (Article 6, VI, LGPD).
- **Lawful basis for processing**
Processing of personal data may only occur if in accordance with one of the lawful bases provided by Article 7 (for regular personal data) or Article 11 (for sensitive personal data) of the LGPD.
- **Purpose limitation**
The purpose principle requires personal data to be processed for legitimate, specific and explicit purposes duly informed to the data subject, without any subsequent processing in a manner incompatible with such purposes (Article 6, I, LGPD).
- **Data minimisation**
Data minimisation is linked to the necessity principle. Personal data must be processed to the minimum

extent necessary for achievement of the respective data processing purposes (Article 6, III, LGPD).

- **Proportionality**

The proportionality principle relates to the necessity principle and thus also to data minimisation. Personal data must be processed using pertinent, proportional, non-excessive data. The type and amount of data processed must be in accordance with the intended purpose (Article 6, II and III, LGPD).

- **Retention**

Personal data shall be eliminated at the end of their processing, within the scope and technical limits of the activities, but may be retained for the following purposes: (i) fulfilment of statutory or regulatory obligations by the controller; (ii) studies by research bodies, ensuring, whenever possible, the anonymisation of personal data; (iii) transfer to a third party, to the extent that the data processing requirements set forth in the LGPD are fulfilled; or (iv) exclusive use by the controller, provided they may not be accessed by a third party, and to the extent that the data are anonymised (Article 16, LGPD).

- **Accuracy**

Data subjects shall be assured of accurate, clear, relevant and up-to-date data, to the extent necessary and for achievement of the purposes for which they are processed (Article 6, V, LGPD).

- **Adequacy**

Personal data shall be processed in a manner consistent with the purposes informed to the data subject, taking into consideration the context of such processing (Article 6, II, LGPD).

- **Free Access**

Data subjects shall be assured of the right to make easy and free-of-charge inquiries into processing mechanisms and duration, as well as the integrity of their personal data (Article 6, IV, LGPD).

- **Security**

Technical and administrative measures shall be adopted to protect personal data from unauthorised access and from accidental or unlawful events of destruction, loss, change, communication or dissemination of such data (Article 6, VII, LGPD).

- **Prevention**

Preventive measures shall be adopted to avoid damage from processing of personal data (Article 6, VIII, LGPD).

- **Non-discrimination**

Personal data cannot be processed for discriminatory purposes, i.e., in an unlawful or abusive manner (Article 6, IX, LGPD).

- **Liability and accountability**

The processing agents shall evidence the adoption of effective measures capable of demonstrating unnecessary compliance with personal data protection rules, as well as the effectiveness of such measures (Article 6, X, LGPD).

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to (copies of) data/information about processing**
The right of access to personal data consists of making available or providing to the data subject copies of his or

her personal data processed by the controller (Articles 18, II, and 19, LGPD). The response for the access request can be made online or in writing by delivering the data to the data subject in hard copy.

There are two ways of responding to data access requests, depending on the request submitted by the data subject: (i) by means of a simplified statement, including a summary of the main personal data processed by the controller, provided immediately; and (ii) by means of a complete statement, which must also include the summary referred above, the origin of the data, the lack of records, the criteria adopted for data processing and its purpose, with due regard for trade and industrial secrets, provided within 15 days from the date of the request.

- **Right to rectification of errors**

The right to rectification of incomplete, inaccurate or outdated data consists of correcting any errors concerning personal data of the data subject (Article 18, III, LGPD).

- **Right to deletion/right to be forgotten**

There are two hypotheses of a data subject's right to deletion in the LGPD, as follows:

- (i) The LGPD provides in Article 18, IV, the data subject's right to anonymisation, blocking or erasure whenever the controller is processing his or her personal data in an unnecessary or excessive manner or in violation of the LGPD. Anonymising refers to the use of reasonable and available techniques by which the personal data can no longer be directly or indirectly associated with the data subject. Blocking refers to the temporary suspension of any processing operation carried out with the personal data, keeping the data stored on the controller's database or systems, including an indication that they cannot be used for any other purposes. Erasing refers to removing from the controller's database or systems the personal data, regardless of the procedure being adopted.
- (ii) The LGPD provides in Article 18, VI, that when withdrawing his or her consent for the processing of personal data, the data subject may also request their erasure, with some exceptions as established by Article 16 (e.g., in case of the need to retain the information for compliance with legal or regulatory obligations).

There is no rule on the general right to be forgotten in the LGPD.

- **Right to object to processing**

Article 18, paragraph 2, of the LGPD provides that the data subject has the right to object to the processing of his or her personal data when based on one of the consent waiver events, in the event of non-compliance with the law.

The right to objection consists of ceasing the processing of personal data and suspending further processing activities, i.e., ceasing any further use of the personal data of this data subject.

Additionally, ANPD issued a guide on the practical use of the legitimate interest lawful basis, in which it is stated that the data subject has the right to oppose to the processing of his or her personal data based on the legitimate interest if the data subject believes his legitimate expectations have not been met.

- **Right to restrict processing**

Please see right to deletion above.

- **Right to data portability**

The right to data portability to another service or product supplier consists of providing a copy of the personal

data concerning a data subject to another company, excluding, however, information deemed as business secrets (Article 18, V, LGPD).

The ANPD is expected to regulate the portability right in the near future.

- **Right to withdraw consent**

The right to withdraw consent consists of ceasing data processing carried out on the basis of prior consent, and suspending further processing activities (Article 18, IX, LGPD), i.e., ceasing any further use of the personal data being processed on the basis of the data subject's consent. In most cases, withdrawal of consent will result in the agreement with the data subject being terminated. The consent may be withdrawn at any time upon express notice of the data subject, via free-of-charge and easily accessible procedures.

The withdrawal of consent, however, does not affect processing activities carried out before withdrawal, and in many cases the personal data will continue to be processed if there is another applicable legal basis – for example, events in which personal data should be maintained for compliance with legal obligations.

- **Right to object to marketing**

The right to object to marketing is not explicitly provided by the LGPD. Please refer to the “right to object to processing” right above.

- **Right protecting against solely automated decision-making and profiling**

The data subject has the right to request a review of decisions based solely on automated processing of personal data that affect his or her interests, including decisions intended to define his or her personal, professional, consumption and credit profile or the traits of his or her personality (Article 20, LGPD).

Fulfilment of a request for a review of decisions based on automated processing consists of providing clear and appropriate information concerning the criteria and procedures used for the automated decision, with due regard for trade and industrial secrets.

Differently from data protection laws from other jurisdictions, the LGPD does not explicitly require that the review of decisions based on automated processing include human participation.

- **Right to complain to the relevant data protection authority(ies)**

The data subject has the right to file a petition to the ANPD (Article 18, paragraph 1, LGPD).

- **Right to confirmation**

The right to confirmation of processing consists of informing the data subject on whether the company processes his or her personal data (Article 18, I, LGPD).

There are rare cases where the request is limited solely to confirmation as the data subject usually wishes to have access to his or her personal data as well.

- **Right to be informed about the consequences in case of refusal to consent**

When the controller uses consent as a lawful basis for processing personal data, the data subject has the right to be informed about: (i) the possibility of refusing consent, where feasible; and (ii) the consequences of refusal, which will typically mean the impossibility of using a certain product or service (Article 18, VIII, LGPD).

- **Right to anonymisation or blocking data processing**

Please see “right to deletion” above.

- **Right to request information about data sharing**
Article 18, VII of the LGPD ensures the data subject the right to know with which public and private entities the controller has shared his or her personal data.

5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

Yes. Article 22 of the LGPD provides that data subjects have the right to exercise their rights in court, whether individually or collectively, which could be made through not-for-profit organisations, to the extent all the requirements provided by Brazilian laws are met.

6 Children's Personal Data

6.1 What additional obligations apply to the processing of children's personal data?

The LGPD establishes that children and teenagers' data must be processed in their best interest. Children are individuals from zero to 12 years old (incomplete) and teenagers are individuals from 12 to 18 years old (incomplete).

In May 2023, the ANPD published the Statement CD/ANPD No. 1/2023, which provides that the processing of personal data of children and teenagers can be relied on any lawful basis, provided for in Articles 7 and 11 of the LGPD, and it does not require the consent in every case.

However, if the controller relies on consent to process children's data, the LGPD provides that such consent must be given by a parent or legal guardian in a specific and conspicuous way.

Although not provided in the LGPD, the ANPD sees children, teenagers and elderly people as vulnerable data subjects and therefore requires additional caution from controllers and processors when processing their personal data.

Additionally, it is important to note that other governmental bodies intend to regulate the processing of minors' personal data. This is the case of the National Council for the Rights of Children and Adolescents ("CONANDA"), which published Resolution No. 245/2024 that addresses children and adolescents' rights in virtual environments. For the purpose of Resolution No. 245/2024, "virtual environments" means any information or communication technology, such as: digital networks, content, services and applications available on the Internet; devices and connected environments; virtual and augmented reality; artificial intelligence ("AI"); robotics; and automated systems, biometrics, algorithmic systems and data analysis.

Although there are discussions on whether the CONANDA are purely guidelines or should be interpreted as law, as well as on the unconstitutionality and violation and conflict of laws, Resolution No. 245/2024 establishes specific data protection requirements, such as the prohibition of processing minors' personal data for commercial purposes, such as profiling in connection with consumption, behaviour, and market segmentation and targeted advertisement.

Irrespective of CONANDA's resolutions, the ANPD has ongoing investigation proceedings regarding processing of children and teenagers' personal data.

7 Registration Formalities and Prior Approval

7.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

No, currently there is no obligation on businesses to register with or notify the ANPD in respect of processing activities.

The LGPD simply provides that controllers and processors must keep records of processing activities (Article 37, LGPD); however, it does not impose obligations on registry of such records.

7.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

This is not applicable; please see above.

7.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

This is not applicable; please see above.

7.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

This is not applicable; please see above.

7.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

This is not applicable; please see above.

7.6 What are the sanctions for failure to register/notify where required?

This is not applicable; please see above.

7.7 What is the fee per registration/notification (if applicable)?

This is not applicable; please see above.

7.8 How frequently must registrations/notifications be renewed (if applicable)?

This is not applicable; please see above.

7.9 Is any prior approval required from the data protection regulator?

This is not applicable; please see above.

7.10 Can the registration/notification be completed online?

This is not applicable; please see above.

7.11 Is there a publicly available list of completed registrations/notifications?

This is not applicable; please see above.

7.12 How long does a typical registration/notification process take?

This is not applicable; please see above.

8 Appointment of a Data Protection Officer

8.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

According to Article 41 of the LGPD, the controller has the obligation to appoint a DPO; and, on the other hand, according to Resolution CD/ANPD No. 18/2024 issued by ANPD (which approves the regulation on the role of DPO), the data processor does not have the obligation to appoint a DPO, although the appointment could be considered as a good practice.

- **Small Processing Agents.** In the Resolution CD/ANPD No. 2/2022 on small processing agents, the ANPD determined that small processing agents are not obligated to appoint a DPO; however, the appointment of a DPO by a small processing agent would be considered as good practice, which is likely to be considered as a mitigating factor in case of a sanctioning proceeding (Article 11, Resolution CD/ANPD No. 2/2022).

Resolution CD/ANPD No. 18/2024 also provided for the obligation to appoint a substitute for the DPO, for cases in which the DPO is absent for any reason.

8.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

As the appointment of a DPO is mandatory in some circumstances, if a DPO is not appointed, the failure to appoint can be interpreted as a violation of the LGPD.

A violation of the LGPD may result in the following administrative penalties (in addition to civil liabilities): (i) warnings; (ii) fines up to 2% of the revenues earned by the legal entity, group or conglomerate in Brazil in the preceding year, net of taxes, capped at R\$50 million per offence; (iii) daily fines; (iv) disclosure of the offence; (v) blocking of the personal database to which the offence refers, until the processing activity is corrected; (vi) elimination of the personal data to which the offence refers; (vii) partial or total suspension of the operation of the database to which the offence refers for a maximum

period of six months, extendable for the same period; (viii) suspension of the processing of personal data to which the infringement refers for a maximum period of six months, extendable for the same period; and (ix) partial or total prohibition of the performance of any activities relating to data processing.

According to Resolution CD/ANPD No. 4/2023, the definition of which administrative sanctions will be applicable in cases of violation of the LGPD will depend on: (i) the classification of the infraction as “minor”, “medium” or “serious”; and (ii) the ANPD’s understanding of the proportionality of the sanction in relation to the infraction committed.

On November 2024, the ANPD initiated an investigatory proceeding against 20 companies for not appointing a DPO, not disclosing the DPO information or not providing a communication channel to data subjects. ANPD notified the companies to adequate the information of the DPO. On April 2025, the investigatory proceeding was concluded since all the 20 companies complies with the ANPD’s requirements and were deemed to be in compliance with the LGPD.

In view of these precedents, in the specific case of failure to appoint a DPO, ANPD may impose a warning or require the company to nominate a DPO within a certain deadline.

8.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

Neither the LGPD nor the Resolution CD/ANPD No. 18/2024 provides for specific clauses regarding disciplinary measures or other employment consequences for the DPO. The absence of an express civil liability regime regarding the DPO in the LGPD does not exempt the DPO from the fulfilment of legal obligation, such as labour, contractual and civil.

The liability of the DPO will vary according to the DPO’s role in the company’s organisation. For example, in case the DPO is a statutory director, its liabilities would be similar to those of the statutory directors of limited liability companies; in case the DPO is a non-statutory director, its liabilities would be limited to specific liabilities of employees; and in case the DPO is a third party hired to act as DPO, its liabilities would be those specified in the agreement.

However, Resolution CD/ANPD No. 18/2024 made it clear that the DPO role does not attract personal liability to the DPO for companies’ non-compliance with the LGPD.

8.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

Resolution CD/ANPD No. 18/2024 allows the DPO to perform multiple roles and carry out their activities for more than one data controller, provided that they are able to fully meet their responsibilities related to each controller and that no conflict of interest exists.

8.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The LGPD does not require specific requirements or certifications for the DPO role. Resolution CD/ANPD No. 18/2024 provides that the DPO may be: (i) a natural person, a member of the organisational framework of the processing agent or external to it; or (ii) a legal entity.

However, Resolution CD/ANPD No. 18/2024 provides that the DPO must be able to communicate in Portuguese with the ANPD and data subjects.

Article 7 of the regulation approved by Resolution CD/ANPD No. 18/2024 states that the company that appoints the DPO is responsible for determining the required qualifications for the DPO.

8.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

According to the LGPD, the DPO has the following duties: (i) intermediate the communication between the company and data subjects; (ii) intermediate the communication between the company and the ANPD, and implement any relevant measures arising from such communication; (iii) educate the company's employees and contractors regarding data protection practices; and (iv) perform other attributions determined by the company or by complementary rules, not yet provided by the ANPD.

In addition to such provisions, Resolution CD/ANPD No. 18/2024 provides that supplementary duties of the DPO include assisting the processing agent in relation to: (i) drafting communication regarding personal data security incidents; (ii) drafting the record of personal data processing operations; (iii) drafting the data protection impact assessment; (iv) identification and analysis of risks related to personal data processing; (v) definition of technical and administrative security measures to protect personal data from unauthorised access and from accidental or unlawful situations of destruction, loss, alteration, communication, or any form of improper or unlawful processing; (vi) implementation of internal policies and procedures to ensure compliance with the LGPD and ANPD regulations; (vii) analysis of contractual clauses with third parties regarding personal data protection; (viii) international data transfers; (ix) creation and implementation of good practices and governance rules, and a privacy governance programme; (x) carrying out privacy by design analysis in products and services; and (xi) other activities and strategic decision-making regarding processing of personal data.

8.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

The DPO must be appointed through a formal document, i.e., through a written, dated and signed document. However, such appointment does not need to be registered or notified to the relevant authorities; the full name and contact details of the DPO must, on the other hand, be made publicly available, as described in question 8.8 below.

8.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

Article 41, paragraph 1 of the LGPD provides that the identity and contact information of the DPO must be publicly, clearly and objectively disclosed, preferably on the company's website.

Resolution CD/ANPD No. 18/2024 reinforces such provision and provides that the identity information must cover, at least: (i) the full name of the DPO, if the DPO is a natural person; or (ii) the corporate name or title of the establishment, as well as the full name of the natural person responsible for the entity, if the DPO is a legal entity.

9 Appointment of Processors

9.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

The LGPD does not have any requirements for businesses to enter into any form of agreement with their processors and the ANPD has not yet issued any requirements or regulated this topic.

Notwithstanding the lack of specific legal requirement, it is highly recommended for businesses to enter into agreements with their processors in order to establish the parties' compliance with the LGPD and any other data protection rules, the extent of the parties' responsibilities and liabilities within the scope of their activities under contract, the measures to be taken in case of a data breach, collaboration in relation to the fulfilment of the data subject's rights, mechanisms applicable in case of cross-border data transfer, the obligation to retain or delete information stored by data processors, and effects of the contract termination, among other obligations.

9.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The LGPD does not provide for any requirements for businesses to enter into any form of agreement with their processors, as explained above.

10 Marketing

10.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

Currently, there is no specific general regulation on the sending of electronic direct marketing; however, there are laws and regulations applicable to the matter: (i) the Brazilian Consumer Protection Code; (ii) the LGPD; (iii) regulation issued by the National Telecommunications Agency ("Anatel"); and (iv) state laws for "do-not-spam".

The Brazilian Consumer Protection Code does not contain any specific provision regarding direct marketing actions; however, it establishes several obligations to the advertisers and suppliers that are applicable to such actions. Among other obligations, messages should have an opt-out option to give the consumer the option to stop receiving direct marketing messages.

The LGPD requires a lawful basis to process data. There are discussions regarding the lawful bases that would be applicable to such practices, mainly consent or legitimate interest would apply.

Anatel has issued regulation related to the delivery of marketing via short message service ("SMS") and massive phone calls. Anatel's rules apply in principle to mobile carriers only. Among other requirements, an opt-in must be obtained, an opt-out option must be offered, and information must be clear and detailed.

Under the state laws for "do-not-spam", consumers are given the option to add their contact details to a "do-not-spam" list.

The data subjects with contact details in that list must not be contacted with marketing content, be it phone calls, SMS and, in some cases, even email. The scope may vary with each state.

10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

There is no specific general regulation on the sending of electronic direct marketing in a business-to-business context. In any case, state laws for “do-not-spam” as provided above shall apply for business-to-consumer marketing.

10.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

Currently, there is no specific general regulation on the sending of electronic direct marketing. Please refer to question 10.1 above for a general overview of the Brazilian regulatory system.

Restrictions may apply in other specific scenarios. The Brazilian Bank Federation and the Brazilian Bank Association developed a self-regulation system for payroll-linked loans. In this system, bank clients may opt to not be contacted about payroll-linked loans.

Anatel decided for the creation of a “non-disturbance” national list for consumers who do not wish to receive calls offering specific products and services (such as telecommunication services and payroll-deductible loan or credit card offering).

In 2021, Anatel issued Act No. 1,0413/2021, now replaced by Act No. 13,762/2022, which approved the Operating Procedures for the Assignment of Numbering Resources, by which it became mandatory for the companies that perform telemarketing activities to adopt the allocation of the non-geographic code (CNG) 0303, prohibiting, for this purpose, the use of any other codes. This way, consumers can identify the originator of the call and decide whether to attend the call.

On September 4, 2024, through Act No. 12.712, Anatel expanded the use of 0303, determining that companies that make more than 10,000 daily calls must adopt the prefix, effective from March 2025. According to the Act, companies that make more than 10,000 calls per day and that do not comply with the new rules will have their calls blocked.

Additionally, mechanisms such as opt-outs are recommended as good practice for businesses whenever the company relies on legitimate interest and not on consent in relation to marketing activities.

10.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?

The above-mentioned provisions are applicable to any marketing communication made in the Brazilian territory or whenever there is a consumer relationship regulated by Brazilian law. In relation to the LGPD, it clearly establishes an extraterritorial reach as provided in the answer to question 3.1 above.

10.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

Considering there is no specific restriction on marketing established by the ANPD, the ANPD may verify if marketing activities are carried out in accordance with the LGPD.

The first enforcement decision issued by the ANPD was directed to a telemarketing company that processed personal data without a proper lawful basis. The penalty for such violation of the LGPD was a fine in the total amount of 2% of the company’s revenue per offence.

10.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Although there is no prohibition in the law on the purchase of marketing lists from third parties, the ANPD’s first enforcement decision was related to the provision of marketing lists for electoral candidates. In view of this, if a company is willing to receive marketing lists from third parties, it is recommended that the company ensures the third party complies with data protection laws and regulation, as well as the company itself assessing whether such data processing, in that specific case, is lawful.

10.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Non-compliance with the applicable laws may result in sanctions and penalties that will depend on the type of violation. In case of violation of the LGPD, specific administrative penalties are provided in Articles 52 to 54 (as detailed in the answer to question 8.2); in case of violation of the Brazilian Consumer Protection Code, penalties therein provided shall apply. Notwithstanding the foregoing, individual and collective lawsuits could be filed due to alleged violation of data privacy or consumer rights, seeking for indemnification for material and moral rights.

11 Cookies

11.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

Differently from the European Union, cookies or similar tracking technologies are not regulated in Brazil by a specific rule/regulation.

On October 18, 2022, the ANPD published on its website a Guide on Cookies and Personal Data Protection (“Cookies Guidelines”), which aim to provide processing agents with good practices related to the subject. The Cookies Guidelines present conceptual issues about cookies and similar tracking technologies, dividing them into categories (e.g., first-party cookies, third-party cookies, necessary cookies and non-necessary cookies, among other classifications).

The Cookies Guidelines also discuss the recommended legal bases for the processing of personal data through cookies and similar tracking technologies, which should be defined according to the categories of cookies. The guidelines further recommend that processing agents develop a cookie policy, which may be presented: (i) as a specific section in the privacy

policy; (ii) in a specific and separate location; or (iii) in the cookie banner itself, provided that the cookie policy contains clear, precise and easily accessible information on the data processing.

Finally, the Cookies Guidelines provide instructions on how to design cookie banners, including indications of: (i) how the data subjects' rights should be presented; (ii) what information should be present; (iii) how the data subjects can manage cookies; and (iv) what should be avoided when designing the banners.

11.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

As explained above, there are no specific restrictions applicable to cookies, but only specific guidance issued by the ANPD.

The Cookies Guidelines provide for the following types of cookies:

- (i) First-party or primary cookies: are cookies directly defined by the website or app that the data subject is visiting. Generally, primary cookies cannot be used to track activity in a website other than the original website in which they were put. This type of cookie can include information such as login credentials, shopping cart items or preferred language.
- (ii) Third-party cookies: are cookies created by a domain other than the one that the data subject is visiting. They derive from functionalities of other domains that are embedded on a website, as in the display of adverts.
- (iii) Necessary cookies: are those used for the website or app to carry out basic functions or correctly operate. For this reason, the collection of information is essential to ensure functioning of the website or for proper provision of services. Therefore, the activities addressed as strictly necessary include those related to a specific functionality of the service.
- (iv) Non-necessary cookies: are cookies that do not fall within the definition of necessary cookies and disabling these cookies will not impair functioning of the website or app or use of services by users. Within this context, non-necessary cookies are related to non-essential functionalities of the service, app or website.
- (v) Analytical or performance cookies: collect data and information about how users use the website, which pages they more frequently visit on that website, the occurrence of errors, or information about the performance of the website or app.
- (vi) Functionality cookies: are used to provide basic services requested by users and allow to remember preferences of the website or app, such as the user name, region or language.
- (vii) Marketing cookies: are used to collect the data subject information with the purpose of displaying adverts. More specifically, from the collection of information about the user's browsing habits, the marketing cookies allow their identification, the building of profiles and the display of personalised adverts.
- (viii) Session or temporary cookies: are designed to collect and store information while data subjects access a website. They are usually deleted after the end of a session.
- (ix) Persistent cookies: the data collected by cookies are stored and may be accessed and processed by the controller for a definite period, which may vary from some minutes to multiple years.

According to the ANPD's examples set forth in the Cookies Guidelines, the "consent" lawful basis is the appropriate lawful basis for non-necessary cookies. On the other hand, the "legitimate interest" lawful basis is the appropriate lawful basis for necessary cookies.

11.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

The ANPD has not yet taken any enforcement action in relation to cookies.

11.4 What are the maximum penalties for breaches of applicable cookie restrictions?

As provided above, there is no specific regulation on cookies or similar technologies and therefore there are no specific penalties for breaches of restrictions. However, it is expected that all processing of personal data through cookies complies with the LGPD.

In case a processing activity related to the use of cookies is in violation of the LGPD, the administrative penalties described in question 8.2 may apply, in addition to complaints or lawsuits filed by other authorities or the data subject itself.

12 Restrictions on International Data Transfers

12.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

The transfer of personal data to other jurisdictions is only permitted in accordance with the instances set forth by the LGPD, such as: (i) for cross-border transfers to third countries or international organisms with adequate protection on the same level as established by the LGPD (a list of countries will be issued by ANPD); (ii) transfers that are necessary for international legal cooperation among intelligence, investigation and prosecution bodies; (iii) transfers that are necessary to protect the life or physical integrity of the data subject(s) or others; (iv) transfers authorised by the ANPD; (v) transfers under international cooperation agreements; (vi) transfers that are necessary for executing or enforcing public policies or public services; (vii) transfers with the specific consent of the data subject; (viii) transfers that are necessary for the fulfilment of a legal or regulatory obligation, for the execution of a contract or preliminary procedures relating to a contract to which the data subject is a party, on the request of the data subject, or for the regular exercise of rights in the course of judicial, administrative or arbitration proceedings; and (ix) when the controller ensures safeguards through the use of specific contractual clauses, standard contractual clauses ("SCCs"), global corporate clauses, seals, certificates or codes of conduct.

On August 23, 2024, the ANPD enacted Resolution CD/ANPD No. 19/2023, which establishes the Regulation on International Data Transfers, pursuant to Articles 33–36 of the LGPD. The Regulation on International Data Transfers outlines the rules and procedures for recognising the adequacy of foreign countries or international organisations and sets forth contractual mechanisms for the international transfer of personal data.

Among the mechanisms regulated are the SCCs, which define the minimum safeguards and conditions required for

international data transfers. Data controllers and processors relying on SCCs must incorporate the ANPD-approved clauses into their contractual instruments by August 23, 2025. The template (Portuguese and English versions) of the SCCs is available on ANPD's website.

The regulation also provides for the possibility of using specific contractual clauses and global corporate rules ("BCRs"). BCRs apply to intra-group international data transfers and require prior approval from the ANPD. These rules must include, among other elements, a commitment to implement a privacy governance programme, a description of the international transfers covered by the BCRs, the identification of the destination countries, and a list of the entities within the corporate group to which the rules apply.

Specific clauses may be adopted in exceptional cases where it is demonstrably unfeasible to use the SCCs. These must ensure an equivalent level of data protection to that provided by the SCCs and must be tailored to the particularities of the transfer operation. Such clauses must be approved by ANPD.

Please note that in case of federal administrative public entities, restrictions to the storage of data outside Brazil may apply.

Sectorial rules may impose requirements to the storage of data outside Brazil in the financial market, such as BCB Resolution No. 304/2023, applicable to all financial market system operating institutions (as detailed in question 1.3 above) and the cybersecurity regulation that applies to entities regulated or authorised by the BCB (Resolution No. 4,893/2021 and Resolution No. 85/2021).

12.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

Please refer to the response to question 12.1. above. The most-used mechanism is SCCs.

12.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

International transfers do not require registration/notification or prior approval from the national authority. However, approval from the ANPD is one of the legal instances set forth by the LGPD that allows international transfers.

12.4 Do transfers of personal data to other jurisdictions require a transfer impact assessment? If conducting a transfer impact assessment is only mandatory in some circumstances, please identify those circumstances.

There is no legal requirement to draft a transfer impact assessment for international transfer of personal data. Regardless, whenever the international transfer is deemed as a high-risk activity, the controller must fill out a data protection impact assessment (applicable to any and all high-risk data processing activity).

According to Resolution CD/ANPD No. 2/2022, a processing activity will be considered as a high-risk activity when it cumulatively meets at least: (i) general criteria; and (ii) specific criteria.

General criteria are: (i) processing on a large scale (i.e., when processing involves a significant number of data subjects, also considering the volume of data involved, as well as the duration, frequency and geographical scope of the processing); or (ii) processing that may significantly affect data subjects' interests and rights (i.e., when the processing may prevent the exercise of rights or the use of a service, as well as cause property or moral damage to the data subjects, such as discrimination, violation of physical integrity, of the right to image, and reputation, financial fraud or identity theft).

A processing activity will meet a specific criterion whenever the processing involves: (i) monitoring or control of public accessible areas; (ii) automated processing; (iii) emerging or innovative technologies; or (iv) sensitive data or children's, adolescents' and elderly's data.

12.5 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?

No official guidance has been issued by the authorities in Brazil.

12.6 What guidance (if any) has/have the data protection authority(ies) issued in relation to the use of standard contractual/model clauses as a mechanism for international data transfers?

As mentioned above, the Regulation on International Data Transfers includes the official SCCs for international data transfers under the LGPD, available here in English: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/regulation-on-international-transfer-of-personal-data.pdf>

These SCCs, detailed in Annex II of the Regulation on International Data Transfers, establish minimum safeguards and conditions for lawful cross-border transfers of personal data. To be valid, the SCCs must be adopted in full, without modification, either as standalone agreements or as annexes to broader contracts, provided that no other provisions contradict or alter their content.

The Regulation on International Data Transfers mandates that data controllers and processors utilising SCCs must incorporate the ANPD-approved clauses into their contractual instruments by August 23, 2025. Additionally, the regulation requires controllers to provide data subjects with access to the full text of the SCCs upon request within 15 days and to publish clear, accessible information about international data transfers on their websites.

Furthermore, the ANPD's regulation allows for the recognition of foreign SCCs as equivalent to the Brazilian SCCs, subject to a formal approval process before ANPD. Interested parties may request such recognition by submitting the foreign clauses, translated into Portuguese, along with relevant legislation and a compatibility analysis with the LGPD. The ANPD will assess whether the foreign clauses ensure a level of data protection equivalent to that guaranteed by the national SCCs and consider the potential impacts on international data flows and diplomatic relations. Once approved, these equivalent

clauses will be published on the ANPD's website and can be used as valid mechanisms for international data transfers.

13 Whistle-blower Hotlines

13.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

The Anticorruption Law in Brazil (Law No. 12,846/2013) and its related Decree No. 8,420/2015 include the existence of a whistle-blower hotline as a parameter for the integrity programme of a company. The whistle-blower hotline must be open to all employees and third parties, be widely advertised, and must have protection mechanisms for the whistle-blowers in good faith. The current legislation does not specify or limit the permitted scope for the hotline.

13.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous reporting is encouraged as one of the protection mechanisms, as mentioned in guidelines issued by the *Controladoria Geral da União*.¹

14 CCTV

14.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

No. The use of CCTV currently does not require registration, notification and/or prior approval from the ANPD. However, as the use of CCTV involves the processing of personal data, the controller must comply with the LGPD's principles and obligations and ensure all reasonable technical and administrative security measures are taken to guarantee the protection of the data, including the implementation of a privacy governance.

As provided in question 12.4 above, monitoring or control of public accessible areas is one of the specific criterion to identify a high-risk activity. In view of this, whenever using CCTV, companies must verify if any general criteria is met to evaluate if the processing activity is deemed as a high-risk activity and therefore requires a data protection impact assessment.

In addition, there are local and regional laws to guide and determine the adoption of additional procedures, such as those referring to the affixing of signs indicating the filming procedures; for example, São Paulo's Municipal Law No. 13,541/2003, which provides for the placement of a visible sign about filming environments and Decree No. 43,236/2003, which regulates such Municipal Law.

14.2 Are there limits on the purposes for which CCTV data may be used?

Neither the LGPD nor the ANPD have specifically regulated limits on the purposes for which CCTV data may be used. However, as any other processing activity, the use of CCTV

data must follow the LGPD's principles and obligations. Therefore, the process must be: (i) for legitimate, specific and explicit purposes, of which the data subject is informed; (ii) compatible with the purpose notified to the data subject; (iii) limited to the minimum necessary for the achievement of the purpose of which the data subject is informed; (iv) clearly notified to the data subject; (v) protected against unauthorised use or access by technical and administrative measures; and (vi) conducted in such a way that prevents discrimination.

15 Employee Monitoring

15.1 What types of employee monitoring are permitted (if any), and in what circumstances?

The LGPD does not regulate employee monitoring and the ANPD has not yet provided any specific guidance or regulation regarding this subject. However, under Brazilian labour legislation, employers have the ability to determine how employees should render their services as well as behave in the workplace. This ability, which is commonly referred to as "employers' directive power", may include: (i) monitoring the company's email address provided to the employee; (ii) supervising the type of information and/or content that employees should not have access to while using company's devices (e.g., private or improper material); (iii) creating and implementing general rules on how the company's devices should be used if owned and granted by the company to employees for the rendering of services (e.g., must not be taken home, should not be used for personal purposes, etc.); and (iv) placement of a CCTV system.

Therefore, if the monitoring activity can be justified by a lawful basis provided by the LGPD and is not in violation of the law (specifically privacy rights), it may be performed by the employers. It is important to note that controllers (employers) must keep records of all personal data processing in a manner that it is able to demonstrate compliance with the LGPD, adopt technical and organisational security measures to protect personal data from unauthorised access and from accidental events or unlawful destruction, loss, modification, communication, dissemination or any other occurrence arising from improper or unlawful processing, and provide data subjects with sufficient information regarding the processing activities.

15.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

The consent of the employee is not always required since there are other legal bases that could justify the processing activities related to employee monitoring, such as the regular exercise of rights in case of judicial, administrative or arbitral proceedings, execution of the employment agreement and legitimate interest, depending on the purposes of the processing. If the processing involves sensitive data, the adequate legal bases could be the regular exercise of rights in contracts and in case of judicial, administrative or arbitral proceedings, or ensuring fraud prevention and safety of data subjects in identification and record authentication proceedings in electronic systems, depending on the purposes of the data processing.

However, to comply with the LGPD principles, the data controllers (employers) must give transparency to the data subjects (employees) on the processing of their personal data. This means that the controller must inform the data subject of the personal data being processed and the purposes of such processing among other things, such as the data subjects' rights regarding these personal data.

This can be carried out through a general privacy notice providing all processing activities with employees' personal data, or through specific privacy notices according to the monitoring activity being performed; for instance, when providing employees with a company phone or computer devices.

15.3 To what extent do works councils/trade unions/ employee representatives need to be notified or consulted?

Currently, there is no regulation indicating that work councils, trade unions and/or employee representatives should be notified or consulted for the employer to perform employee monitoring.

15.4 Are employers entitled to process information on an employee's attendance in office (e.g., to monitor compliance with any internal return-to-office policies)?

Yes. At the time of writing, there is no restriction on the monitoring of employees' attendance in office, provided the processing activity is carried out in accordance with the LGPD.

16 Data Security and Data Breach

16.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Yes. The security of personal data is not only an obligation, but also a principle in the LGPD (Articles 6, VII, 46 and 50 of the LGPD). It is necessary for all parties involved in the processing of personal data (controllers and/or processors) to ensure and adopt technical and administrative measures to protect personal data from unauthorised access and from accidental or unlawful events of destruction, loss, change, communication or dissemination of such data.

16.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Yes. Article 48 of the LGPD establishes that the data controller must notify the ANPD and the data subjects about the occurrence of a security incident that may result in risks or relevant damages to the data subjects.

In line with LGPD obligation, Resolution CD/ANPD No. 15/2024 (on the security incident notification proceeding) states that the controller has the obligation to notify the ANPD about the occurrence of a security incident that may result in risks or relevant damages to the data subjects within three business days from the date the controller became aware that the security incident involved personal data. Resolution CD/ANPD No. 15/2024 provides in Articles 4 and 5 the interpretation of the requirements to an incident to configure an event that may result in risks or relevant damages to the data subjects.

Communication to the ANPD must be carried out through a specific system of the ANPD (known as SUPER/ANPD) and must include all the information required in a specific form

available by ANPD, including: (i) the description of the nature and category of personal data affected; (ii) the number of affected data subjects, breaking down, where applicable, the number of children, adolescents or elderly people; (iii) the technical and security measures used to protect personal data, implemented before and after the incident, observing commercial and industrial secrets; (iv) the risks related to the incident with identification of possible impacts on data subjects; (v) the reasons for the delay, in case the communication was not carried out within the expected deadline; (vi) the measures that have been or will be adopted to reverse or mitigate the effects of the incident on the data subjects; (vii) the date of occurrence of the incident, when possible to determine, and the date of its knowledge by the controller; (viii) information on the DPO or whoever represents the controller; (ix) identification of the controller and, if applicable, a statement that it is a small processing agent; (x) processor identification, when applicable; (xi) description of the incident, including the main cause, if it is possible to identify it; and (xii) the total number of data subjects whose data is processed in the processing activities affected by the incident.

If controller does not have all the information, it can submit a preliminary communication on the data breach within the three business days, and a complementary version of the communication within 20 business days.

16.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Yes. As provided above, Article 48 of the LGPD provides for the controller obligation to notify the data subjects of the occurrence of a security incident that may result in risks or relevant damages to the data subjects. Resolution CD/ANPD No. 15/2024 provides in Articles 4 and 5 the interpretation of the requirements to an incident to configure an event that may result in risks or relevant damages to the data subjects. Whenever the controller communicates the ANPD, it will have to communicate the data subjects, as the same requirements will apply to both cases (obligation to notify ANPD and data subjects).

Resolution CD/ANPD No. 15/2024 states that data subjects must also be notified of the security incident within three business days from the date the controller became aware that the security incident involved personal data.

Communication to the data subject must include, at least: (i) the description of the nature and category of personal data affected; (ii) the technical and security measures used to protect data, observing commercial and industrial secrets; (iii) the risks related to the incident with identification of possible impacts on data subjects; (iv) the reasons for the delay, if the communication was not made within the deadline; (v) the measures that have been or will be implemented to reverse or mitigate the effects of the incident, when applicable; (vi) the date of knowledge of the security incident; and (vii) a contact for obtaining information and, when applicable, the contact details of the DPO.

16.4 What are the maximum penalties for personal data security breaches?

The LGPD does not provide for specific penalties applicable to a data breach. The ANPD reviews the circumstances of

the data breach in order to confirm if a violation to LGPD has occurred or not in the specific event. In any case of violation of the LGPD, specific administrative penalties are provided in Articles 52 to 54 (as detailed in the answer to question 8.2). In addition, other competent authorities may investigate the incident (such as the Public Prosecutor Office) and/or individuals/entities representing individuals that suffered damages may file claims before Courts.

17 Enforcement and Sanctions

17.1 Describe the enforcement powers of the data protection authority(ies).

- (a) **Investigative powers:** The ANPD has administrative powers to apply sanctions and thus requires a proper prior investigation. The sanctions shall be applied after conclusion of an investigative proceeding and commencement of an administrative sanctioning proceeding that gives the offender the opportunity of full defence, in a gradual, isolated or cumulative form, according to the features of the concrete case, and considering the lawful parameters and criteria. The ANPD may apply precautionary measures in the beginning of the investigation.
- (b) **Corrective powers:** The ANPD has administrative powers to apply sanctions determined by the LGPD, such as: (i) warning, with indication of a deadline for the adoption of corrective actions; (ii) blocking of the personal data to which the offence refers, until the processing activity is regularised; (iii) erasure of the personal data to which the offence refers; (iv) partial suspension of the database to which the infringement refers for a maximum period of six months, extendable for the same period, until the processing is regularised by the controller; (v) suspension of the processing of personal data to which the infringement refers for a maximum period of six months, extendable for the same period; (vi) partial or total prohibition on data processing activities; and (vii) disclosure of the offence after the occurrence thereof has been duly investigated and confirmed.
- (c) **Authorisation and advisory powers:** The ANPD is responsible for the issuance of technical opinions and recommendation.
- (d) **Imposition of administrative fines for infringements of specified legal provisions:** Among the possible applicable sanctions by the ANPD in case of violation of the LGPD, there are administrative fees such as: (i) a one-off fine of up to 2% of the revenues earned by the legal person, group or conglomerate in Brazil in the preceding year, net of taxes, capped at R\$50 million per offence; and (ii) a daily fine, subject to the cap referred to above.
- (e) **Non-compliance with a data protection authority:** In case of non-compliance with the ANPD's binding rules, the offender could be subject to the same sanctions described above. In addition, in case of non-compliance with the ANPD's decision, daily fines could be applicable as established by the LGPD.

17.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

Some of the administrative sanctions to be applied by the ANPD stated in the LGPD provide for the suspension of the

processing of personal data and partial or total prohibition on data processing activities. The application of these sanctions does not require a court order and can be imposed by ANPD.

17.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

The ANPD is still focusing on its educational powers, by way of issuing public consultations and calls for contribution for the issuance of guidelines and regulations.

However, the ANPD has initiated its sanctioning processing in July 2023. The ANPD has disclosed a list of nine sanctioning proceedings that are currently in place. Only one sanctioning procedure relates to a private legal entity, as described below.

On July 6, 2023, the ANPD issued its first decision in the context of an administrative proceeding against a private entity, regarding violation of the LGPD by a telemarketing company, which allegedly sold phone numbers of electors in the context of electoral campaigns. The company's infraction allegedly consisted in the lack of: (i) applicable lawful basis for its processing activities; (ii) appointment of the DPO; and (iii) collaboration with the ANPD's requests. The ANPD's decision resulted in the imposition of administrative sanctions (warning and fines up to 2% of the company's revenue).

In addition, the ANPD is currently conducting several high-profile enforcement actions under the LGPD. These include supervisory procedures against:

- a social media network company for alleged violations related to the processing of children's and adolescents' personal data – specifically regarding the platform's failure to implement adequate age verification mechanisms; and
- a messaging company to evaluate whether its data-sharing practices comply with transparency and consent requirements under the LGPD.

The ANPD has also initiated sector-wide investigations, including:

- Data protection practices in the pharmaceutical industry, particularly focusing on loyalty programmes and personal data use.
- LGPD compliance in the use of facial recognition technologies by 23 football clubs for ticketing and stadium access.

Most recently, the ANPD ordered a company to suspend alleged incentives linked to the processing of data, citing risks to fundamental rights.

These cases demonstrate the ANPD's expanding oversight across both private and public sectors, demonstrating its focus on supervisory actions before initiating sanctioning procedures.

17.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

Yes, the ANPD has already filed investigations against business established in other jurisdictions that provides products and services to Brazilian users, and collects data from Brazilian users. In one of the cases, the ANPD has imposed a precautionary measure to make it to cease part of its activities.

18 E-discovery/Disclosure to Foreign Law Enforcement Agencies

18.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

The Brazilian Code of Civil Procedure does not provide for a broad discovery phase, as it occurs, for example, in the U.S. Therefore, the scope and depth of disclosure will mostly rely on a case-by-case analysis, that will take into account the facts and concrete elements of the case and the fulfilment of the basic legal requirements for the discovery.

Brazil has declared, under Article 23 of the Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, that it will not execute letters of request (letters rogatory) issued for the purpose of obtaining pre-trial discovery of documents. In spite of that, the Superior Court of Justice has executed certain letters rogatory on pre-trial discovery under the understanding that the aforementioned declaration “is not to block the search for evidence abroad, but to prevent abuse” (CR 13559-US). Once again, a case-by-case analysis will be necessary.

18.2 What guidance has/have the data protection authority(ies) issued on disclosure of personal data to foreign law enforcement or governmental bodies?

Currently, there is no guidance from the ANPD regarding e-discovery requests or requests for disclosure from foreign law enforcement agencies.

19 Artificial Intelligence

19.1 Are there any limitations on automated decision-making involving the processing of personal data using artificial intelligence?

Under Brazilian law, particularly Article 20 of the LGPD, data subjects have the right to request a review of decisions made solely through automated processing of personal data (using AI or not), that affect their interests. This includes decisions related to creditworthiness, professional profile, consumer behaviour, or other aspects of their personality. Additionally, controllers shall provide, if requested by the data subject, clear and adequate information on the criteria and procedures used in automated decision-making processes, while preserving commercial and industrial secrecy.

To clarify the scope and practical implementation of these safeguards, the ANPD conducted a public consultation between November 2024 and January 2025, focusing on the automated processing of personal data and the use of AI. Following this initiative, the ANPD consolidated the contributions and published Technical Note No. 12/2025/CON1/CGN/ANPD, which sets out preliminary interpretations and regulatory considerations.

19.2 What guidance (if any) has/have the data protection authority(ies) issued in relation to the processing of personal data in connection with artificial intelligence?

In addition to Technical Note No. 12/2025/CON1/CGN/ANPD mentioned above, ANPD released the third volume of

its “Technology Radar” series, titled “Generative Artificial Intelligence”,² providing an in-depth analysis of generative AI models and their implications for data protection.

Also, in August 2024, the ANPD lifted the preventive suspension previously imposed on a social network platform regarding the use of personal data for training its generative AI systems. This decision followed the social network platform’s submission of a Compliance Plan, which includes several commitments to align its data processing activities with the LGPD. Key measures outlined in the plan involve enhancing transparency through clear notifications to users about data processing for AI training and providing simplified mechanisms for users and non-users to opt-out.

20 Trends and Developments

20.1 In your opinion, what enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.

Over the past 12 months, enforcement activity under the LGPD has increased. While the ANPD began imposing administrative penalties in 2023 – primarily targeting public entities, which are not subject to monetary fines under Resolution CD/ANPD No. 4/2023 – a growing trend involves closer scrutiny of the private sector and the tech industry. Notably, on July 6, 2023, the ANPD issued its first sanction against a private entity: a very small telemarketing company found to have processed voter data without legal basis. The company was sanctioned for failing to appoint a DPO (Article 41), lacking an appropriate legal basis (Article 7), and not cooperating with the ANPD (Article 5 of Resolution No. 1/2021). Sanctions included a warning and two monetary fines.

In 2024, enforcement actions became increasingly focused on high-profile cases involving complex data processing practices. For example, the ANPD investigated social media network platform’s use of personal data for training generative AI systems. Following a preventive suspension, the social media network was only permitted to resume data use after submitting a compliance plan.

In 2025, additional enforcement initiatives targeted facial recognition practices by football clubs, data practices in the pharmaceutical retail sector, and loyalty programmes, as well as alleged incentives tied to data processing activity.

These cases indicate a probable enforcement trend: the ANPD is moving beyond foundational compliance to scrutinise emerging technologies, especially in contexts involving children, biometric data and AI.

20.2 In your opinion, what “hot topics” are currently a focus for the data protection regulator?

The ANPD has identified several key focus areas for 2025–2026, as outlined in its Regulatory Agenda, reflecting a growing effort to address emerging technologies and high-impact data processing practices.

One of the central topics is the regulation of AI and automated decision-making. The ANPD aims to clarify the scope and application of Article 20 of the LGPD – particularly concerning data subjects’ rights in the context of automated decisions – and to develop rules on the governance and legal bases applicable to AI-driven data processing.

Another major area of focus is the protection of children’s and adolescents’ personal data. The ANPD intends to issue

specific rules on parental consent and age verification in digital environments, aligned with international standards such as the OECD Recommendation on Children in the Digital Environment.

Additionally, the ANPD plans to address the legal basis for credit protection activities. The regulatory agenda includes the development of specific guidance on the interpretation and operationalisation of Article 7, section X, of the LGPD, which provides for data processing when necessary to ensure the protection of credit.

Other hot topics include detailed regulations on data subject rights (such as access, correction, deletion and portability), the implementation of Data Protection Impact Assessments for high-risk processing, technical and administrative security measures, biometric data processing, and data sharing by public authorities.

As of 2025, Brazil is actively advancing a regulatory framework for AI through Law Bill No. 2,338/2023 (“AI Bill”), introduced by Senator Rodrigo Pacheco. The AI Bill was approved by the Federal Senate in December 2024, following significant input from multiple sectors and the Internal Temporary Committee on Artificial Intelligence, and is currently under review in the House of Representatives.

Endnotes

- 1 Available at: <https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/integridade/arquivos/programa-de-integridade-diretrizes-para-empresas-privadas.pdf>
- 2 Available here in English: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/radar-tecnologico-inteligencia-artificial-generativa-versao-em-lingua-inglesa.pdf>



Larissa Galimberti specialises in technology, licensing, data protection and intellectual property law. With a focus on cutting-edge technologies, digital platforms and the sharing economy, Larissa brings a wealth of expertise in navigating complex legal matters in the rapidly evolving tech landscape. Her proficiency in software, data analytics, IoT, cybersecurity, media and entertainment, as well as her adeptness in handling agreements involving intellectual property rights, make her an invaluable asset in safeguarding the interests of Brazilian and international clients.

Pinheiro Neto Advogados

Rua Hungria, 1100, Jardim Europa
São Paulo, SP
Brazil

Tel: +55 11 3247 6265

Email: lgalimberti@pn.com.br

LinkedIn: www.linkedin.com/in/larissagalimbertiafonso



Luiza Fonseca de Araujo assists national and international clients in the advisory sphere, focusing on topics related to technology, data protection, AI and intellectual property. She has experience in structuring digital platforms, product development, adapting activities to data protection legislation, administrative proceedings with the National Data Protection Authority, and regulatory analysis related to AI.

Pinheiro Neto Advogados

Rua Hungria, 1100, Jardim Europa
São Paulo, SP
Brazil

Tel: +55 11 3247 6331

Email: laraujo@pn.com.br

LinkedIn: www.linkedin.com/in/luiza-araujo



Cecília Alberton Coutinho Silva is a lawyer specialised in technology, with a focus on the global regulatory and transactional spheres such as data protection, crypto assets, blockchain, AI and cybersecurity. She holds a Master's degree in Law and Technology from Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS), with research on facial recognition and regulatory modalities by private entities. Currently, she assists companies in leveraging technology across its various aspects, providing innovative legal solutions to drive business growth while ensuring compliance with regulations in Brazil and Latin America.

Pinheiro Neto Advogados

Rua Hungria, 1100, Jardim Europa
São Paulo, SP
Brazil

Tel: +55 11 3247 8553

Email: ccoutinho@pn.com.br

LinkedIn: www.linkedin.com/in/cec%C3%ADlia-coutinho-781a2a15a

Pinheiro Neto Advogados has rendered counsel in virtually all areas of legal practice since 1942 and is structured to offer its clients comprehensive assistance with all legal aspects of their business activities. It currently has over 840 members, including more than 100 partners, approximately 380 associates, in addition to a team of paralegals and professionals in other support areas. Pinheiro Neto Advogados provides services to approximately 2,000 local and international groups and has full-service offices in São Paulo, Rio de Janeiro and Brasília, as well as representative offices in Palo Alto and Tokyo.

www.pinheironeto.com

PINHEIRONETO
ADVOGADOS

China

King & Wood Mallesons



Susan Ning



Han Wu

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

There are three major principal laws on data protection, i.e., the Cybersecurity Law (“**CSL**”), the Personal Information Protection Law (“**PIPL**”) and the Data Security Law (“**DSL**”).

1.2 Is there any other general legislation that impacts data protection?

Yes. Both the general civil and criminal legislation in China provide requirements on data protection.

In particular, the Civil Code, which took effect on 1 January 2021, establishes the right to privacy and the principles of personal information protection. It mainly provides a definition of personal information and sets out basic requirements for personal information processing, the obligations on the personal information handlers and the rights of individuals to their personal information. Most of the provisions in the Civil Code are restatements of requirements contained in the CSL. National Standards such as the Information Security Technology – Personal Information Security Specification (“**Standard**”) also have an impact on the authorities’ enforcement on data protection practices.

The Criminal Law also sets forth offences relating to infringing personal data and privacy, e.g., the offence of infringing citizens’ personal information in Article 253-(1), the offence of refusing to fulfil information network security responsibilities in Article 286-(1), and the offence of stealing, purchasing or illegally disclosing other people’s credit card information in Article 177-(1). The Interpretation of Several Issues Regarding Application of Law to Criminal Cases of Infringement of Citizen’s Personal Information Handled by the Supreme People’s Court and the Supreme People’s Procuratorate issued in 2017 provides further explanation regarding the offences relating to infringing personal data and privacy.

1.3 Is there any sector-specific legislation that impacts data protection?

Yes. There are various pieces of sector-specific legislation that impact data protection, including but not limited to medical and health, telecommunications, e-commerce, automobiles, and the industry and information technology sector. For

example, the Commercial Bank Law requires banks to keep confidential information on depositors’ personal savings deposit businesses. The People’s Bank of China (“**PBOC**”) has released the Implementing Measures of the PBOC for Protection of Financial Consumers’ Rights and Interests, which provide basic requirements on protection of financial information (including personal information) of individual customers. The Biosecurity Law and the Administrative Regulations on Human Genetic Resources set out requirements on processing of human resource information. The E-commerce Law restates the principle of personal information protection in the field of e-commerce industry. There are also various legal requirements on protection of personal information and data in the automobile industry, such as the Several Provisions on Automotive Data Security Management (for Trial Implementation). Furthermore, the Provisions on Protecting the Personal Information of Telecommunications and Internet Users set out the obligations of telecommunication and Internet information service providers. Last but not the least, the Data Security Management Measures of Industry and Information Technology Sector cover the applicable laws, data classification, special protection, data life cycle compliance and other requirements towards the data processing activities in the field of industry and information technology. Additionally, regulators in charge of natural resources, financial services, transportation, banking and insurance and other areas have issued data security administrative measures, aiming to provide sectoral regulations on data protection.

1.4 What authority(ies) are responsible for data protection?

As for personal information protection, China has no single authority responsible for enforcing provisions.

The Cyberspace Administration of China (“**CAC**”) is responsible for coordinating the protection of personal information and relevant supervision and administration work, while other departments of the State Council, such as the Ministry of Industry and Information Technology (“**MIIT**”), the public security department and other relevant departments are responsible for the supervision and administration of personal information protection in their respective sectors.

For example, the Ministry of Public Security (“**MPS**”) and its local branches are entitled to impose administrative penalties and are also in charge of criminal investigations against the unlawful obtaining, sale or disclosure of personal information.

The MIIT and its local branches are responsible for the supervision and administration of personal information in the telecommunications and Internet sector.

Also, the State Administration for Market Regulation (“SAMR”) and its local counterparts are responsible for the supervision and administration of personal information of consumers, pursuant to the Law on Protection of the Rights and Interests of Consumers.

There are also industry-specific data protection requirements, which are mainly enforced by relevant industry authorities. For example, the PBOC and the China Banking and Insurance Regulatory Commission promulgate and enforce legal requirements on the protection of personal financial information. The National Health Commission and Ministry of Science and Technology supervise the processing of medical and health data.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **“Personal Data”**
Pursuant to the PIPL, personal data/personal information refers to all kinds of information related to identified or identifiable natural persons recorded by electronic or other means, excluding information that has been anonymised.
- **“Processing”**
Pursuant to the PIPL, the processing of personal information includes the collection, storage, use, processing, transmission, provision, disclosure and deletion, etc. of personal information.
- **“Controller”**
The PIPL does not use the term “controller(s)” to refer to entities that hold or handle personal information. Instead, it names such entities as “personal information handlers” considering their engagement in processing personal information. Pursuant to the PIPL, a personal information handler is defined as an organisation or individual that independently determines the purpose and method of the processing of personal information.
- **“Processor”**
The PIPL does not define “processor” in the same way as under the General Data Protection Regulation (“GDPR”). However, the PIPL sets out the scenario of entrusted processing of personal information, where a personal information handler may entrust an entity with such processing.
- **“Data Subject”**
The PIPL does not define “data subject”. However, both the Civil Code and the PIPL provide that a natural person’s personal information shall be protected by law. It is widely understood that a natural person/individual identified by the personal information shall be regarded as a data subject.
- **“Sensitive Personal Data”/“Special Categories of Personal Data”**
Pursuant to the PIPL, sensitive personal data/sensitive personal information refers to personal information that is likely to result in damage to the personal dignity of any natural person or damage to his or her personal or property safety once disclosed or illegally used, including such information as biometric identification, religious belief, specific identity, medical health, financial

account and whereabouts, as well as the personal information of minors under the age of 14.

- **“Data Breach”**
The CSL, PIPL and DSL do not define “data breach”. The National Contingency Plan for Cyber Security Incidents issued by the CAC defines “Cybersecurity incidents”, which refers to incidents that cause harm to the network and information systems or data therein and adversely affect society due to human factors, hardware or software defects or failures, natural disasters, etc. Cybersecurity incidents can be divided into hazardous programme incidents, network attack incidents, information destruction incidents, information content security incidents, equipment and facility failures, catastrophic incidents and other incidents.
- **Other key definitions:**
 - **“De-identification”** refers to the process in which personal information is processed so that it is impossible to identify certain natural persons without the aid of additional information.
 - **“Anonymisation”** refers to the process in which personal information is processed so that it is impossible to identify certain natural persons and cannot be recovered.
 - **“Network data”** refers to various electronic data processed and generated through networks.

3 Territorial and Material Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

Under the CSL, relevant authorities are entitled to monitor, prevent and manage cybersecurity risks and threats from other jurisdictions. Pursuant to Article 50, if any information from other jurisdictions is found to be prohibited by law, the CAC and competent authorities may take measures to block the transmission of such information. Pursuant to Article 75, the law applies to an overseas institution, organisation or individual that engages in activity that also endangers Critical Information Infrastructure (“CII”). Further, companies operating under the offshore model but providing services to Chinese clients/users may also be subject to the personal data protection rules established by the CSL, especially those on the cross-border transfer of data. However, the law does not clearly specify how to realise the sanctions. As such, the extent to which these provisions will be enforced abroad against overseas companies remains unclear.

The PIPL provides similar rules to the GDPR regarding its jurisdiction over businesses located outside of China. Article 3 provides that the law shall apply to the processing of personal information of natural persons who are in China under any of the following circumstances, where the processing happens outside of China:

- 1) where the purpose is to provide domestic natural persons with products or services;
- 2) where the activities of domestic natural persons are analysed and evaluated; and
- 3) other circumstances as prescribed by laws and administrative regulations.

Furthermore, according to Article 42 of the PIPL, where an overseas organisation or individual engages in personal information processing activities that infringe upon the personal

information rights and interests of citizens of the People's Republic of China ("PRC") or endanger the national security and public interests of the PRC, the CAC may include such organisation or individual in the list of subjects to whom provision of personal information is restricted or prohibited, announce the same, and take measures such as restricting or prohibiting provision of personal information to such organisation or individual.

The DSL also empowers relevant authorities with the power to investigate the liabilities of entities that process data outside of China that damages the national security, public interest or the legitimate rights and interests of citizens and organisations.

3.2 Do the data protection laws in your jurisdiction carve out certain processing activities from their material scope?

The PIPL does not apply to the processing of information that has been anonymised, meaning that the information can no longer be linked back to an identified or identifiable individual and this process cannot be reversed. Additionally, the PIPL does not apply to processing activities by individuals for the purpose of purely personal and family issues.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

■ Transparency

Article 41 of the CSL stipulates that network operators shall make public the rules for collecting and using personal data, and expressly notify the purpose, methods and scope of such collection and use. The same principle has also been included in the PIPL. According to Article 7: the principles of openness and transparency shall be observed in the processing of personal information; the rules for the processing of personal information shall be publicly disclosed; and the purpose, manners and scope of processing shall be explicitly indicated.

■ Lawful basis for processing

Article 41 of the CSL and Article 1035 of the Civil Code require network operators to abide by the "lawful, justifiable and necessary" principles when collecting and using personal information. The PIPL similarly requires that the processing of personal information shall follow the principles of lawfulness, legitimacy, necessity and good faith, and processing personal information by misleading, fraud, coercion or otherwise is not permitted.

Furthermore, Article 13 of the PIPL provides various legal grounds for the processing of personal information, including:

- 1) the consent of the individual concerned is obtained;
- 2) it is necessary for the conclusion or performance of a contract to which the individual concerned is a party, or for the implementation of human resource management in accordance with the labour rules and regulations formulated in accordance with the law and the collective contract concluded in accordance with the law;
- 3) it is necessary for the performance of statutory duties or statutory obligations;

- 4) it is necessary for the response to a public health emergency or for the protection of the life, health and property safety of a natural person in an emergency;
- 5) personal information is processed within a reasonable scope to conduct news reporting, public opinion-based supervision and other activities in the public interest;
- 6) processing within a reasonable scope of personal information that is publicly disclosed in accordance with the PIPL; or
- 7) other circumstances prescribed by laws and administrative regulations.

■ Purpose limitation

Article 41 of the CSL requires that network operators shall not collect any personal information that is not related to the services it provides. The PIPL similarly requires that the processing of personal information shall be for a definite and reasonable purpose and be directly related to the purpose of processing.

■ Data minimisation

Article 6 of the PIPL provides that the processing of personal information shall be conducted in a way that minimises the impact on personal rights and interests, and shall be limited to the minimum scope for achieving the purpose of processing. It is prohibited to excessively collect personal information.

■ Proportionality

There is no explicit rule providing for a "proportionality principle" under the CSL or the PIPL, but the data minimisation principle under the PIPL is similar in essence to the "proportionality principle", emphasising "processing of personal data only within a proper and necessary scope", and "shall be conducted in a way that minimises the impact on personal rights and interests".

■ Retention

Pursuant to Article 19 of the PIPL, unless otherwise stipulated by laws and administrative regulations, the retention period of personal information shall be the minimum period necessary for achieving the purpose of processing.

■ Accuracy

Article 8 of the PIPL provides that the quality of personal information shall be ensured in the processing of personal information to avoid the adverse impact on personal rights and interests caused by inaccurate or incomplete personal information.

■ Accountability

Article 9 of the PIPL requires a personal information handler to be responsible for its processing of personal information and take necessary measures to ensure the security of the personal information processed.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

■ Right of access to (copies of) data/information about processing

Both the Civil Code and the PIPL entitle an individual to consult or copy his/her personal information from a personal information handler.

■ Right to rectification of errors

The PIPL provides that where an individual finds that his/her personal information is inaccurate or incomplete,

he/she is entitled to request the personal information handler to make corrections or supplements. The Civil Code and the CSL provide similar rules.

■ **Right to deletion/right to be forgotten**

The PIPL requires a personal information handler to delete personal information actively or under the request of relevant individuals in any of the following circumstances:

- 1) where the purpose of handling has been achieved, it is impossible to achieve such purpose, or it is no longer necessary to achieve such purpose;
- 2) where the personal information handler ceases to provide products or services, or the storage period has expired;
- 3) where the individual withdraws his/her consent;
- 4) where the personal information handler processes personal information in violation of laws, administrative regulations or the agreement; or
- 5) other circumstances stipulated by laws and administrative regulations.

■ **Right to object to processing**

Under the PIPL, a data subject has the right to restrict or refuse others to process his/her personal information.

■ **Right to restrict processing**

Under the PIPL, a data subject has the right to restrict or refuse others to process his/her personal information.

■ **Right to data portability**

Pursuant to Article 45 of the PIPL, where an individual requests to transfer his/her personal information to a personal information handler designated by him/her, which meets the conditions stipulated by the CAC, the personal information handler shall provide a way for the transfer.

■ **Right to withdraw consent**

Article 15 of the PIPL provides that where the processing of personal information is based on the consent of the individual concerned, the individual is entitled to withdraw his/her consent. The personal information handler shall provide a convenient method for the individual to withdraw his/her consent.

■ **Right to object to marketing**

Section 8.4 of the Standard stipulates that data subjects have the right not to receive commercial advertisements that are based on their personal data. Furthermore, regarding marketing by means of automated decision-making, the PIPL requires the processor to provide convenient rejection ways to relevant individuals.

■ **Right protecting against solely automated decision-making and profiling**

The PIPL provides that where a processor makes use of personal information to make an automatic decision, it shall ensure the transparency of the decision-making and the fairness and impartiality of the results, and shall not impose unreasonable discriminatory treatment on individuals in respect of the transaction price and transaction conditions. In a scenario in which there is information pushing and commercial marketing to an individual through automated decision-making, the processor shall in parallel provide options that do not target the individual's personal characteristics, and provide convenient means of rejection to relevant individuals. On the other hand, an individual shall have the right to require the personal information handler to make an explanation and to reject such explanation only through automatic decision-making where such decision has a significant impact on an individual's rights and interests.

■ **Right to complain to the relevant data protection authority(ies)**

The right for individuals to complain to data protection authorities has been recognised in a number of pieces of legislation. For example, Section IX of the Decision of the Standing Committee of the National People's Congress ("NPC") on Strengthening Network Information Protection provides that any organisation or individual has the right to report to the relevant authorities regarding the illegal or criminal conduct of stealing or otherwise unlawfully acquiring, selling or providing to others a citizen's personal electronic information. Further, the CSL provides in Article 14 that one could report acts that endanger network security to the CAC, telecom and public security authorities.

Under the PIPL, any organisation or individual shall have the right to complain or report illegal personal information processing activities to the authorities performing duties of personal information protection.

■ **Right of close relatives of the deceased**

The PIPL protects the rights of close relatives of the deceased. Where a natural person dies, his/her close relatives may, for the purpose of their own lawful and legitimate interests, exercise such rights as consulting, copying, correcting and deleting the relevant personal information of the deceased as prescribed in this chapter, unless otherwise arranged by the deceased prior to his/her death.

5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

There are similar rules under the PIPL. Article 70 of the PIPL provides that where any personal information handler processes personal information in violation of this Law, which infringes upon the rights and interests of a large number of individuals, the People's Procuratorate, the consumer organisations specified by law and the organisations determined by the CAC may bring a lawsuit to a people's court.

6 Children's Personal Data

6.1 What additional obligations apply to the processing of children's personal data?

Under the PIPL, personal information of children under the age of 14 shall be regarded as sensitive personal information, the processing of which shall be subject to additional legal requirements. Pursuant to Article 31 of the PIPL, processing personal information of children under the age of 14 requires the consent of the children's parents or other guardians, and specialised rules shall be formulated for such processing.

Besides, the State Council has issued the Regulation on the Protection of Minors in Cyberspace, and the CAC has promulgated a special regulation regarding the protection of children's personal information, i.e., the Provisions on the Cyber Protection of Children's Personal Information. Among other obligations, data handlers that process children's personal information shall formulate special data protection rules and user agreements and designate persons as responsible for the protection of such information.

7 Registration Formalities and Prior Approval

7.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

Under the CSL, PIPL and DSL, transferring personal information or important data abroad may trigger such obligation in certain circumstances. As for operators of CII (“CIIOs”), a security assessment shall be conducted pursuant to the measures developed by the CAC and/or competent departments of the State Council, if the personal information or important data generated or collected by them within the territory of China needs to be transferred abroad for business purposes. Personal information handlers whose quantity of processing reaches that as prescribed by the CAC will also be subject to such obligation according to the PIPL. As for other personal information handlers, there are some other ways provided by the PIPL to compliantly transfer personal information outside China, among which the data handlers can choose to pass the security assessment organised by the CAC.

Specifically, the Measures for the Security Assessment of Cross-border Data Transfer (“**CBDT Assessment Measures**”) and the Measures for the Standard Contract for the Cross-border Transfer of Personal Information apply to the data handlers’ provision of important data and personal information collected and generated in their operations within the territory of China to overseas recipients. Specifically, if the data handler provides important data abroad, is a CIIO, or reaches certain thresholds in terms of the provision of personal information abroad, the data handler would need to file for the CBDT security assessment with the CAC, unless one of the exemptions enumerated in the Provisions for Promoting and Regulating the Cross-Border Flow of Data applies. If the data handler does not trigger the CBDT security assessment thresholds under the CBDT Assessment Measures, then the data handler may choose to sign the Standard Contract for the Cross-border Transfer of Personal Information (“**Standard Contract**”) with the overseas recipient(s) and file the Standard Contract and Personal Information Protection Impact Assessment report with the provincial CAC to remain compliant, unless one of the exemptions enumerated in the Provisions for Promoting and Regulating the Cross-Border Flow of Data applies.

According to the DSL, handlers of important data shall, in accordance with the relevant provisions, carry out risk assessments on their data processing activities on a regular basis and submit a risk assessment report to the relevant competent authority. On an industrial-specific basis, the CAC has issued a regulation on the security protection of automotive data, in which the CAC requires that an automotive data handler shall conduct risk assessments and submit an assessment report to the cyberspace administration at provincial level and other relevant authorities for its processing of important data. Such handler is further required to submit its annual automotive data security management report to these authorities by 15 December of each year. Furthermore, the international transfer of important data by the handler shall also be subject to the assessment organised by the CAC and relevant authorities. Handlers of important data must report their data disposal plans and recipient details to the relevant authorities if events such as mergers, divisions, dissolutions or bankruptcies occur.

The CAC also sets out legal requirements on the application of algorithm recommendation technologies and deep synthesis for the provision of Internet information services, where an algorithm-recommendation or deep-synthesis service provider with a public-opinion attribute or social mobilisation ability shall go through record-filing formalities.

Additionally, where the processing of data raises national security issues, such activities may further trigger a cybersecurity review. According to the Cybersecurity Review Measures released by the CAC and a number of other national departments, the purchase of network products and services by CIIOs and the data processing activities carried out by online platform operators, which affect or may affect national security, shall be notified to the relevant authorities for cybersecurity review. Online platform operators holding the personal information of more than 1 million users shall also declare for cybersecurity review when they enter into an initial public offering (“**IPO**”) in other countries.

7.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

For the security assessment of international transfer of personal information and important data and the filing of a Standard Contract, the notification is designed to be specific, covering various aspects such as legitimacy, fairness, necessity of the transfer, data elements, quantity, sensitivity of the data, security risk, etc.

The report by automotive data handlers is also required to be specific. Handlers are requested to provide details of the processing activities, such as the type, scale, purpose and necessity of the processing of automotive data, the measures for security protection and management of automotive data, provision of automotive data to third parties, data security incidents and the handling thereof, etc.

The filing of algorithms needs to be conducted via the Internet information service algorithm record-filing system operated by the relevant authorities, where detailed information such as the service provider’s name, service form, application field, algorithm type, algorithm self-assessment report and content shall be provided.

The cybersecurity review is also conducted in a detailed manner. Relevant data handlers need to file (including but not limited to) an assessment report analysing in detail the risk factors concerning national security.

7.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

For international data transfer, the notification should be made by data handlers per “scenario”, which are akin to a business process and may cover several related processing purposes. For security assessment, the notification is valid for three years, unless one of the specified changes occurs, such as changes to processing purposes. For Standard Contract filing, it remains valid unless one of the changes occurs.

For automotive data, each data handler (who conducts important data processing) is required to file a report of its overall automotive data processing activities. Similarly, the filing of algorithms shall be conducted by each relevant

service provider, and if any change occurs to the information filed, the service providers shall make modifications within 10 working days.

As for cybersecurity review, as mentioned above, the review process is initiated when a CIIO purchases network products and services that affect or may affect national security, or when an online platform operator's certain data processing activity affects or may affect national security, or when an online platform operator holding personal information of more than 1 million users enters into an IPO in other countries.

7.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

Please refer to questions 7.1 and 7.3.

7.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

Please refer to question 7.2.

7.6 What are the sanctions for failure to register/notify where required?

CIIOs that fail to notify their cross-border transfer of personal information and important data, according to the CSL, shall be warned and ordered by the competent authority to make rectifications, and shall be subject to confiscation of illegal earnings and a fine ranging from RMB 50,000 to RMB 500,000, and may be subject to a suspension of related business, winding up for rectification, shutdown of website and revocation of business licence, and the supervisor directly in charge and other directly liable persons shall be subject to a fine ranging from RMB 10,000 to RMB 100,000. As for personal information handlers, pursuant to the PIPL, the authorities may order them to make corrections, give a warning to them and confiscate their illegal gains. If they refuse to make corrections, a fine of not more than RMB 1 million shall be imposed; and a fine of not less than RMB 10,000 but not more than RMB 100,000 shall be imposed on the person directly in charge and other directly liable persons. Where the circumstances are serious, such processor may face a higher fine of not more than RMB 50 million or not more than 5% of its turnover of the previous year; the authorities may also order it to suspend relevant business or suspend business for rectification, and revoke the relevant business permit or business licence. Furthermore, a fine of not less than RMB 100,000 but not more than RMB 1 million shall be imposed on the person directly in charge and other directly liable persons, and a decision may be made to prohibit the said persons from acting as directors, supervisors, senior executives and persons-in-charge of personal information protection of relevant enterprises within a certain period of time.

According to the DSL, an important data handler failing to report may face an order to make rectifications and a warning, and may be concurrently fined not less than RMB 50,000 but not more than RMB 500,000, and the person directly in charge and other directly liable persons may be fined not less than RMB 10,000 but not more than RMB 100,000; if the processor refuses to make rectifications or causes serious consequences

such as massive data leakage, it will be fined not less than RMB 500,000 but not more than RMB 2 million, and may be ordered to suspend the relevant business or stop the business for rectification, and the relevant business permit or business licence will be revoked. The person directly in charge and other directly liable persons will be fined not less than RMB 50,000 but not more than RMB 200,000.

With respect to any algorithm recommendation service provider with the attribute of public opinions or the ability to mobilise the public, who has obtained record-filing by concealing relevant information, providing false materials or other improper means, its record-filing shall be revoked, a warning given, or a notice of criticism circulated; if the circumstances are serious, it shall be ordered to suspend information updating and impose a fine of not less than RMB 10,000 but not more than RMB 100,000. For such deep-synthesis service providers, they shall be penalised in accordance with the provisions and administrative regulations for not fulfilling the record-filing duties. If such violation constitutes a crime, the violator may be held criminally liable in accordance with the law.

CIIOs using products and/or services that have not undergone or have failed in the security review shall be ordered by the competent authority to stop such use and shall be subject to a fine equivalent to more than one but less than 10 times the purchase price, and the supervisor directly in charge and other directly liable persons shall be subject to a fine ranging from RMB 10,000 to RMB 100,000.

7.7 What is the fee per registration/notification (if applicable)?

Normally, such notifications are free of charge.

7.8 How frequently must registrations/notifications be renewed (if applicable)?

Please refer to questions 7.1 and 7.3.

7.9 Is any prior approval required from the data protection regulator?

For the international data transfers mentioned in question 7.1, it is widely recognised that prior approval is required, where applicable. As for important data processing, there is no requirement of prior approval in the DSL. The same goes with the filing of algorithms.

For cybersecurity review, it is understood that prior approval is required.

7.10 Can the registration/notification be completed online?

The international transfer and filing of algorithms are conducted online; however, in limited cases, offline is still acceptable. Cybersecurity reviews are offline.

7.11 Is there a publicly available list of completed registrations/notifications?

For algorithm registrations, a list of completed registrations can be found on the Internet Information Service Algorithm

Filing System. For the CBDT security assessments, up until April 2025, the CAC published some completed filings through public channels. It is unclear as to whether and how the CAC would continue publishing the completed registrations.

7.12 How long does a typical registration/notification process take?

For the CBDT security assessment, the regulations provide that the CAC shall complete a security assessment of outbound data within 45 working days commencing from the date of issuing the written notice of acceptance; if the circumstance is complex or supplementary materials are required, the said time limit may be extended appropriately. Standard Contract filing generally takes much less time to complete.

For the filing of algorithms, relevant authorities shall, within 30 working days upon receipt of the complete record-filing materials submitted by the record-filing applicants, grant record-filing, issue record-filing numbers and make public the record-filing; if the materials are incomplete, record-filing shall not be granted, and the record-filing applicant shall be notified, with reasons stated, within 30 working days.

The cybersecurity review follows a period of “30+15+15” working days for an ordinary review procedure. Where a special procedure is needed, the review shall generally be completed within 90 working days, and the time limit may be extended for complicated cases.

8 Appointment of a Data Protection Officer

8.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

Under the PIPL, where the quantity of personal information processed reaches that specified by the CAC, the personal information handler shall designate a person in charge of personal information protection (hereinafter “DPO”) to be responsible for supervising the activities of processing personal information and the adopted protection measures.

In the Administrative Measures for Personal Information Protection Compliance Audits issued in February 2025, the CAC suggested that any personal information handler handling the personal information of more than 1 million people shall designate a DPO.

Under the DSL, handlers of important data shall specify the person(s) responsible for data security and the management body and implement the responsibility of data security protection.

8.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

The PIPL and relevant laws do not directly specify the legal liability of the DPO. However, the laws specify the legal liability of the “directly liable person-in-charge or other directly liable persons” and the statutory duties of those subjects to specify the legal liability of such officers.

Under the PIPL, the authorities may order the processor to make corrections, give a warning to it and confiscate its illegal gains. If it refuses to make corrections, a fine of not more than

RMB 1 million shall be imposed; and a fine of not less than RMB 10,000 but not more than RMB 100,000 shall be imposed on the person directly in charge and other directly liable persons. Where the circumstances are serious, such a processor may face a higher fine of not more than RMB 50 million or not more than 5% of its turnover of the previous year; the authorities may also order it to suspend relevant business or suspend business for rectification, and revoke the relevant business permit or business licence. Furthermore, a fine of not less than RMB 100,000 but not more than RMB 1 million shall be imposed on the person directly in charge and other directly liable persons, and a decision may be made to prohibit the said persons from acting as directors, supervisors, senior executives and persons-in-charge of personal information protection of relevant enterprises within a certain period of time.

According to the DSL, an important data handler failing to appoint a data security officer may face an order to make rectifications and a warning, and may be concurrently fined not less than RMB 50,000 but not more than RMB 500,000, and the person directly in charge and other directly liable persons may be fined not less than RMB 10,000 but not more than RMB 100,000; if the processor refuses to make rectifications or causes serious consequences such as massive data leakage, it will be fined not less than RMB 500,000 but not more than RMB 2 million, and may be ordered to suspend the relevant business or stop the business for rectification, and the relevant business permit or business licence will be revoked. The person directly in charge and other directly liable persons will be fined not less than RMB 50,000 but not more than RMB 200,000.

8.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

If a DPO fails to perform his or her allocated duties with due diligence, then the DPO may be accused of administrative or even criminal liabilities depending the severity of the offence.

8.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

The law and relevant rules do not specify whether a business can appoint a single DPO to cover multiple entities.

8.5 Please describe any specific qualifications for the Data Protection Officer required by law.

Section 11.1 of the Standard specifies that the DPO shall have relevant management experience and professional knowledge of personal information protection.

8.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

Please refer to the response to question 8.1. Furthermore, Section 11.1 of the Standard provides that the DPO’s responsibilities include but are not limited to:

- 1) direct responsibility for, and comprehensive and overall implementation of, the organisation’s personal data security;

- 2) organising the formulation of a personal information protection work plan and supervising its implementation;
- 3) drafting, issuing, implementing and regularly updating the privacy policy and related regulations;
- 4) establishing, maintaining and updating the list of personal data held by the organisation (including the type, amount, origin, recipient, etc. of the personal data) and authorised access policies;
- 5) conducting a personal data security impact assessment, proposing countermeasures and suggestions for personal information protection, and urging the rectification regarding security risks;
- 6) organising personal data security training;
- 7) conducting product or service testing before its release in case of unknown collection, use, sharing and other processing activities of personal data;
- 8) announcing information such as complaint or reporting methods and promptly accepting the complaint and report;
- 9) conducting safety audits; and
- 10) communicating with supervisory authorities, and reporting on personal information protection and incident handling, etc.

8.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

Under the PIPL, yes. The personal information handler shall make public the contact information of the DPO and submit their name and contact information to the authorities.

8.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

Yes, but the disclosure of the DPO's real name is not necessarily required.

9 Appointment of Processors

9.1 If a business appoints a processor to process personal data on its behalf, must the business enter into a form of agreement with that processor?

Yes. Under the PIPL, where a personal information handler entrusts others with the processing of personal information, it shall agree with the agent on the purpose, time limit and method of entrusted processing, type of personal information and protection measures, as well as the rights and obligations of both parties, and supervise the personal information processing activities of the agent. It is noteworthy that, according to the requirements of the PIPL, the entrusted data processing agreement should also include a clause that the entrusted party would assist the processor in fulfilling the compliance obligations specified in the PIPL.

9.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

Please refer to question 9.1.

10 Marketing

10.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

Marketing by email or SMS as a type of commercial advertising are regulated by the Civil Code, the Advertising Law, and other relevant laws and regulations. Article 1033 of the Civil Code stipulates that unless otherwise provided by law or expressly consented to by the right holder, no organisation or individual shall intrude upon another person's private life through making phone calls, sending text messages, using instant-messaging tools, sending emails and flyers, and the like means. Pursuant to Article 43 of the Advertisement Law, no organisation or individual shall, without obtaining the consent or request of the parties concerned, distribute advertisements to them via electronic means. Advertisements distributed via electronic means shall state the true identity and contact details of the senders, and the method for the recipients to refuse acceptance of future advertisements. Article 44 further provides that advertisements published in the form of pop-up windows on the website shall show the "close" sign prominently.

Regarding the special provisions on emails, Article 13 of the Administration of Internet Electronic Mail Services provides that the word "advertisement" or "AD" must be indicated in the email subject, and it is prohibited to send emails containing commercial advertisements without the express consent of the receivers. Article 14 provides that if an email recipient who has expressly consented to receive electronic direct marketing subsequently refuses to continue receiving such emails, the sender shall stop sending such emails unless otherwise agreed by the parties. The receivers shall be provided with the contact details for the discontinuation of the receipt of such emails, including the email address of the sender, and shall ensure that such contact details are valid within 30 days.

Regarding the special provisions on SMS, back in 2015, the MIIT issued and implemented the Provisions on the Administration of Communications Short Message Services. Article 18 provides that the providers of SMS and short message content may not send commercial short messages to users without the latter's consent or request, or shall stop sending such short messages to users when the latter clearly present their refusal after their consent.

In addition, according to the Measures for the Supervision and Administration of Online Trading, Article 16 provides that no online trading business may send commercial information to consumers without their consent or request. An online trading business shall, when sending commercial information, expressly indicate its true identity and contact information, and in a prominent manner, provide consumers with simple and convenient methods to refuse subsequent receipt thereof free of charge. In the case of any consumer's explicit refusal, it shall cease sending such information immediately and may not send it again after a change of name.

10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

Current Chinese laws and regulations, including the Advertising Law, the Administration of Internet Electronic

Mail Services Procedures, the Measures for the Supervision and Administration of Online Trading, and the Administration of Communications Short Message Services, do not specify whether they are only applicable to business-to-consumer marketing.

10.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

Several regulations are applicable to situations where the sending of marketing is via other means. For instance, Article 2 of the Internet Advertising Administrative Measures indicates the Advertising Law and these Measures shall apply to commercial advertising activities which directly or indirectly market goods or services, through websites, web pages, Internet application programs and other Internet media, in the form of scripts, images, audio, video or other means, within the territory of the PRC. In this case, the scope of Internet advertising has been expanded, and the sending of marketing via other means (e.g., live broadcast and recommendation) are regulated by this regulation.

Specifically, Article 9 provides that an Internet advertisement shall be identifiable, enabling consumers to identify it as an advertisement. Article 10 provides that an advertiser or advertisement publisher publishing an Internet advertisement in the form of a pop-up, among others, shall distinctively indicate the closing sign to ensure one-click closing. On one hand, the restrictions refine the prohibited situations that affect one-click closing and include open-screen advertisements into the scope of the application. On the other hand, the regulations clarify the prohibited behaviours of deceiving, inducing users to click, and browsing advertisements.

Moreover, Section VII of the Decision of the Standing Committee of the NPC on Strengthening Network Information Protection provides that any organisation or individual shall not send commercial electronic messages to the fixed-line, mobile telephone or email inbox of an electronic message receiver without the prior consent or request of the receivers or if the receivers explicitly express rejection.

The operators of an e-commerce platform, when displaying search results of goods or services, shall mark “advertisement” for bid-ranked products or services, pursuant to Article 40 of the E-commerce Law. Furthermore, Article 18 provides that e-commerce business operators who provide search results based on consumers’ preference or consumption habits shall in the meantime provide options not targeting consumers’ personal characteristics.

As for marketing by means of automated decision-making, the PIPL requires the relevant processor to provide options not specific to individuals’ characteristics simultaneously, or provide methods for individuals to refuse such marketing or push content.

10.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?

The Advertisement Law, the Internet Advertising Administrative Measures, Provisions on the Administration of Internet Pop-up Information Push Services, and the E-commerce Law apply to operators providing products and services within the territory of China, while for foreign operators providing products or services to China on an offshore model, the law does not further elaborate whether it will

apply or not. However, according to Article 3.2 of the CBDT Assessment Measures, business operators not registered in China but providing products or services to China using the Chinese language, making settlement by RMB and delivering products to China are considered to be “providing products or services to China”, in which case it is possible that the relevant provisions will apply.

The PIPL applies to the processing of personal information of natural persons within China for the purpose of providing products or services to them or analysing or assessing their conduct. Therefore, marketing sent by a personal information handler from other jurisdictions could be subject to the PIPL if it falls into the cases above.

10.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

The Administration for Market Regulation is mainly responsible for the enforcement of marketing restrictions. There are recent cases where authorities such as the Administration for Market Regulation are taking action. For example, in 2017, Shanghai Paipaidai Financial Information Service Co., Ltd. was fined RMB 800,000 for its infringement of the Advertisement Law, the breaches including, among others, sending direct advertisements via email without obtaining the prior consent of the recipients.

10.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

If the source of the marketing lists is legitimate and lawful and the data subject has consented, then it is not prohibited. Otherwise, it is illegal to do so, as network service providers and other enterprises, public institutions and their employees are obligated to keep strictly confidential a citizen’s personal electronic information collected during their business activities, and may not disclose, falsify, damage, sell or illegally provide such information to others, as provided in the Decision of the Standing Committee of the NPC on Strengthening Network Information Protection.

10.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Article 63 of the Advertisement Law provides that sending direct marketing communications without obtaining the consent of the target may result in a fine of up to RMB 30,000.

E-commerce platforms that do not clearly mark “advertisement” for bid-ranked products may face a fine of up to RMB 100,000, pursuant to Article 81 of the E-commerce Law and Article 62 of the Advertisement Law.

In addition, Article 77 of the E-commerce Law provides that e-commerce business operators who provide search results in violation of Article 18 as described in question 10.3 shall be ordered to make the correction within a stipulated period, their illegal income shall be confiscated, and a fine ranging from RMB 50,000 to RMB 200,000 may be imposed. In serious cases, a fine ranging from RMB 200,000 to RMB 500,000 should be imposed concurrently.

As for the penalties under the PIPL, please refer to question 8.2.

11 Cookies

11.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

There is no legislation addressing the use of cookies explicitly. Given that cookies may fall within the definition of personal information, it is understood that the general regulations on personal data apply to the use of cookies.

Specifically, for instance, Article 7 of the PIPL provides that personal information shall be processed under the principles of openness and transparency, with the rules of processing personal information in line with the expressly stated purposes, methods and scope of processing. Therefore, the websites using cookies shall disclose what types of personal information would be collected by different cookies and for what purposes, and allow different cookies to be disabled (if not strictly necessary) by the visitors, respectively.

11.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

The law does not distinguish between different types of cookies at this stage.

11.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

There are no administrative actions on the use of cookies. Nonetheless, in 2015, the search engine Baidu's use of cookies to personalise advertisements aimed at consumers when they enter certain third-party websites was found by the court not to infringe an individual's right to privacy. In addition, in 2021, the CAC-lead enforcement on the mobile app-pushed content included the penalty on the abuse of cookies for news and marketing content that may violate the content governance principles.

11.4 What are the maximum penalties for breaches of applicable cookie restrictions?

Please refer to the maximum penalties for other general breaches.

12 Restrictions on International Data Transfers

12.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

The CSL, PIPL and DSL have set out requirements for CBDT. For restrictions on the cross-border transfer of personal information and important data, please refer to questions 7.1–7.12.

In a nutshell, under the PIPL, personal information handlers that have processed personal information reaching the threshold specified by the authorities in terms of quantity and CIIOs shall store the personal information collected and generated within the territory of the PRC. When it is truly necessary for a personal information handler to provide personal information overseas, relevant specific requirements

shall be satisfied (specific requirements are briefly discussed in question 12.2).

Nevertheless, as for general restrictions:

- 1) CBDT is only permitted when it is truly necessary for business purposes;
- 2) the personal information handler shall obtain personal information subjects' separate consent before conducting CBDTs;
- 3) the consent shall be obtained after sufficient notification; for instance, details of CBDT shall be disclosed (i.e., overseas recipients' name and contact information, purpose and method of the processing, types of personal information to be transferred overseas, and the means and procedures for individuals to exercise their rights) to the personal information subjects;
- 4) the Personal Information Protection Impact Assessment ("PIPIA") shall be conducted by the personal information handler in advance, and the personal information processing activities shall be recorded;
- 5) the personal information handler shall ensure that the processing activities of the overseas recipient meet the specified protection standards to conduct CBDTs lawfully;
- 6) in some circumstances, if an overseas recipient does not have a local entity and is defined as a personal information handler located outside of Mainland China, it is required to establish representatives or agencies located inside China to handle affairs relating to personal information protection; and
- 7) the personal information handler and its overseas recipient(s) shall agree on the data security protection responsibilities and obligations in a legal document concluded between the parties.

12.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

Typically, the PIPL and other laws and regulations provide several methods that a business can adopt to compliantly transfer personal information abroad, including the following:

- 1) passing the CBDT security assessment organised by the CAC (for CIIOs and data handlers whose quantity of processing of personal information reaches the threshold prescribed by the CAC);
- 2) obtaining certification by a specialised agency for protection of personal information in accordance with the requirements of the CAC;
- 3) entering into a Standard Contract with the overseas recipient in accordance with the official Standard Contract formulated by the CAC, specifying the rights and obligations of both parties; or
- 4) meeting other conditions prescribed by laws, administrative regulations or the CAC.

12.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

The Provisions for Promoting and Regulating the Cross-Border

Flow of Data, released on 22 March 2024, provide the circumstances under which personal information handlers shall register/obtain approval from the provincial or national CAC.

Generally, the personal information handler must apply for CBDT Security Assessment with the CAC and obtain prior approval if it satisfies any of the following conditions: 1) conducts CBDT activities involving important data; 2) is recognised as a CIIO and conducts CBDT activities involving personal information; or 3) cumulatively provides more than 1 million individuals' personal information (excluding sensitive personal information) or more than 10,000 individuals' sensitive personal information outside of China, counting from 1 January of the current year, while not being a CIIO.

If the personal information handler satisfies the following condition, it is required to file the Standard Contract with the relevant provincial CAC or obtain personal information protection certification: cumulatively provides more than 100,000 but less than 1 million individuals' personal information (excluding sensitive personal information) or less than 10,000 individuals' sensitive personal information outside of China, counting from 1 January of the current year, while not being a CIIO.

In both cases, the personal information handler would need to conduct data-mapping internally regarding its CBDT activities and prepare and submit the application/filing materials in accordance with the guidelines issued by the CAC. Overall, the CBDT Security Assessment process requires more complicated materials and takes longer than the Standard Contract filing process.

12.4 Do transfers of personal data to other jurisdictions require a transfer impact assessment? If conducting a transfer impact assessment is only mandatory in some circumstances, please identify those circumstances.

Please refer to questions 12.1 and 12.3.

12.5 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?

This is not applicable.

12.6 What guidance (if any) has/have the data protection authority(ies) issued in relation to the use of standard contractual/model clauses as a mechanism for international data transfers?

The CAC has issued updated guidance, along with the Provisions for Promoting and Regulating the Cross-Border Flow of Data, providing requirements on the procedure and submission documents for the Standard Contract filing process, in which personal information handlers can also find the templates for the report to be filed. The updated guidance also indicates that filing for Standard Contracts needs to be conducted via the CAC online filing platform; the updated guidance includes the details on the user guide of such online filing platform.

13 Whistle-blower Hotlines

13.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

The PIPL provides that any organisations and individuals shall have the right to file complaints or reports about illegal personal information processing activities with relevant authorities. The authorities receiving complaints or reports shall handle them without delay and notify the complainants and informants of the handling results. Similarly, the DSL provides that any individual or organisation shall have the right to file complaints or reports to relevant authorities. The CSL provides that Internet operators shall establish systems for complaints and reports related to cybersecurity and publish the channels through which complaints and reports may be made.

13.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

There is no provision in the PIPL, DSL or CSL that explicitly prohibits anonymous reporting. Anonymous reporting is generally permitted.

14 CCTV

14.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

Public Security Video Image Information System Administrative Regulations (hereinafter the “**CCTV Regulations**”), which were issued by the MPS and regulate the use of CCTV for public safety purposes, set out three categories of locations:

- locations that may require the installation of CCTV for public safety purposes (such as customs, airports, highways, public spaces like convention centres, etc.);
- locations where the installation of CCTV is prohibited (such as interior spaces within hotels, dormitories, restrooms, etc.); and
- locations that are permitted to install CCTV if it is for public safety purposes.

Article 14 of the CCTV Regulations stipulates that anyone who uses CCTV for public safety purposes (under the first category above) must notify and file with the provincial public security department the type of camera, location of the camera installed, storage period of video images, etc. within 30 days after putting CCTV into use.

There are also several local governments that published regulations on CCTV, and these local regulations are all in force. For example, in Beijing, the Measures of Beijing Municipality for Administration of Image Information Systems for Public Security were published, and Article 11 of it provides that any units that use CCTV for public security shall file a report for

record on the construction of the CCTV for public security within 30 days from the date of completion of construction of relevant CCTV.

14.2 Are there limits on the purposes for which CCTV data may be used?

Pursuant to Article 16 of the CCTV Regulations, it is prohibited to obtain state secrets, trade secrets and personal information from a public security video image information system, or infringe on citizens' privacy by using such a system. Organisations that have been entrusted to undertake the design, construction, inspection, acceptance inspection and maintenance of a public security video system shall keep confidential the video image information and relevant archival materials accessed by them, shall not use the same for any activities unrelated to the entrusted task, and shall not retain, process, divulge or provide the same to others without authorisation.

According to Article 22 of the CCTV Regulations, if the video image information collected by CCTV is used for public dissemination in accordance with the law, which may damage the lawful rights and interests of an individual or any organisation, strict protection measures must be taken against such sensitive personal information, such as faces or motor vehicle plate numbers involved, as well as such information as the name and business licence of a legal person or unincorporated organisation.

According to Article 25 of the CCTV Regulations, investigative, procuratorial and judicial powers, public security and national security organs, as well as the administrative departments of the government at or above town level, may inspect, copy or retrieve the basic information or data collected through CCTV for the purpose of law enforcement, responding to the incident or fulfilment of their lawful authority.

In addition, the CCTV Regulations stipulate that the instalment and use of CCTV must also focus on the personal privacy and personal data interests, reasonably determine the installation position, angle and collection of the scope of the image capturing, set clear warning signs of the use of CCTV, the storage period of the video image captured via CCTV shall be at least 30 days, and after 30 days, if the purpose of processing the video image has been achieved, such video image shall be deleted.

It is worth noting that the PIPL provides restrictions on image capturing and personal identification equipment installed in public places. Such data collection activities shall be necessary for maintaining public security, comply with the relevant provisions of the State, and conspicuous prompting signs shall be set up. An individual's personal image and personal identification information collected may only be used for the purpose of maintaining public security and shall not be used for any other purpose, except with the individual's separate consent.

15 Employee Monitoring

15.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Article 8 of the Labour Contract Law provides that employers are entitled to know about basic information of the worker in direct relation to the labour contract between them; therefore, some types of employee monitoring are permitted, though no

specific rule explicitly addresses employee monitoring. On the other hand, it is prudent that the monitoring does not infringe the employee's privacy.

Moreover, workplace monitoring is an important scenario for the protection of employees' personal data. For instance, in practice, enterprises may achieve business-related goals by means of monitoring employees' browsers, data flow, cushions, toilet time and mobile phones, etc., to prevent the leakage of data or trade secrets, and to supervise whether the employees are working effectively during working hours. In addition, CCTV could commonly be seen around the workplace.

Only when the compliance requirements are met, will the above monitoring activities not violate the employees' personal privacy.

15.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

According to the PIPL, consent may not be needed if the processing of personal information is necessary for the implementation of human resource management in accordance with the internal labour rules and regulations and the collective contract concluded. While the processing of employees' personal information exceeds the human resource management scope, consent is still needed unless the processing falls in other legal bases as prescribed in Article 13 of the PIPL.

In practice, employers usually choose to add a provision in the labour contract or in the employee handbook or similar documents to inform employees of the processing of their personal information, and where necessary, to obtain their consent.

15.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

Article 4 of the Labour Contract Law requires employers to discuss with the employee representatives' congress or all employees, and negotiate with trade unions or employee representatives when formulating, revising or deciding on matters directly involving the vital interests of workers such as remuneration, working hours, rest periods and days off, labour safety and health, insurance and welfare, staff training, labour discipline and labour quota administration, etc. Article 43 further provides that employers shall notify the trade union when they unilaterally rescind a labour contract. However, such notifying or negotiating circumstances may not directly relate to employers' monitoring or processing of employees' personal data.

15.4 Are employers entitled to process information on an employee's attendance in office (e.g., to monitor compliance with any internal return-to-office policies)?

If consent has been obtained from such employee, and the data processing activity is of necessity and legitimacy, then the answer would be yes. Nevertheless, if the employer attempts to process such information without obtaining consent, it may go with another legal ground, for instance, during the period when COVID-19 was striking, employers might be able to process such personal information under the legal basis of "necessary for the response to a public health emergency or for the protection of the life, health and property safety of a

natural person in an emergency". In spite of this, it is worth noting that whether an employer could process an employee's information on a legal ground other than consent shall be assessed on a case-by-case basis.

16 Data Security and Data Breach

16.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

The answer is yes. The CSL, DSL and the PIPL, as the three basic laws in the field of cyberspace security and data compliance in China, all put forward some general obligations on data security.

- **General Obligations from the CSL**
Under Article 40 of the CSL, network operators are obliged to establish and improve the system for user information protection. Under Article 42 of the CSL, network operators are responsible for taking technical and other necessary measures to ensure the security of personal information they collect.
- **General Obligations from the DSL**
Personal information as a kind of data in a broad sense, is also protected by the DSL. Under Article 27 of the DSL, whoever carries out data (including personal information) processing activities shall establish a secure data security management system throughout the whole process and take necessary measures to ensure data security. Furthermore, to carry out data (including personal information) processing activities by making use of the Internet or any other information network, the aforesaid obligations for data security protections shall be performed on the basis of the graded protection system for cyber security.
- **General Obligations from the PIPL**
The PIPL provides in its Article 9 that the personal information handler shall take necessary measures to ensure the security of the personal information handled. Moreover, Article 51 of the PIPL specifically stipulates what kind of method personal information handlers can take to ensure the safety of personal information, such as formulating internal management systems and operating procedures and taking corresponding technical security measures.

All the above obligations are borne by the personal information controller, which is also known as the personal information handler of the PIPL. However, if a network operator of the CSL or a personal information handler of the PIPL as a controller appoints a third party known as a processor to process personal information on its behalf, it shall ensure that such processor will provide an adequate level of protection to the involved personal information.

16.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

The answer is yes. Similar to general obligations on personal information security, the CSL, DSL and the PIPL all put

forward obligations on reporting data breaches to the relevant authorities.

- **Legal Requirements of the CSL**
Under Article 42 of the CSL, in case of (possible) divulgence, damage or loss of data collected, the network operator is required to take immediate remedies and report to the competent authority.
- **Legal Requirements of the DSL**
Similarly, under Article 29 of the DSL, data controllers shall report to the relevant competent authority in case of data security incidents.
- **Legal Requirements of the PIPL**
Under the PIPL, where personal information has been or may be divulged, tampered with or lost, the personal information handler shall immediately take remedial measures and notify the relevant authorities and the individuals concerned. The notice shall include the following matters:
 - 1) the types, reasons and possible harm of the information that has been involved or may be involved in the divulgence, tampering with or loss of personal information;
 - 2) the remedial measures taken by the personal information handler and the measures that can be taken by the individuals to mitigate harm; and
 - 3) the contact information of the personal information handler.

On 8 December 2023, the CAC issued the Administrative Measures for Cybersecurity Incident Reporting (Draft Exposure, "**Incident Measures**"), which is a milestone in respect of data breach notification, specifying the procedure and requirements of data breach incident reporting. In detail, depending on the category of an incident, the reporting obligation shall be performed within one hour, 24 hours or five working days. In terms of the content to be reported, Article 5 and Annex 2 of the Incident Measures stipulate that it shall at least cover the following matters:

- 1) the name of the entity in which the accident occurred and the basic conditions of the facilities, system and platform in which the accident occurred;
- 2) when and where the incident was discovered or occurred, the category of the incident, the impact and harm caused, the measures that have been adopted and their effects;
- 3) the development trend of the situation and possible further impact and harm;
- 4) a preliminary analysis of the causes of the incident;
- 5) clues required for further investigation and analysis, including information of possible attackers, attack paths and existing vulnerabilities;
- 6) measures to be taken further and matters for which support is requested; and
- 7) the status of protection of the incident site.

16.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Yes, please refer to question 16.2.

Furthermore, according to the PIPL, where the personal information handler has taken measures to effectively

avoid harm caused by divulgence, tampering with or loss of information, the personal information handler may opt not to notify the individuals concerned. If the authorities performing duties of personal information protection believe that harm may be caused, they may require the personal information handler to notify the individuals concerned.

16.4 What are the maximum penalties for personal data security breaches?

The PIPL puts forward a general punishment rule for personal information handlers failing to perform their data protection duties, which shall include the scenario of personal information linkage. Specifically, in terms of violation of personal information protection obligations, the competent authorities are entitled to impose a fine of not more than RMB 50 million or not more than 5% of its turnover of the previous year on the data handler. Moreover, a fine of not less than RMB 100,000 but not more than RMB 1 million shall be imposed on persons directly in charge.

Under Article 64 of the CSL, in case of severe violation, an operator or provider in breach of data security may face fines of up to RMB 1 million (or 10 times the illegal earnings), suspension of a related business, winding up for rectification, shutdown of any website(s) and revocation of a business licence. The persons directly in charge may face a fine of up to RMB 100,000.

In addition, under Article 45 of the DSL, in case of causing serious consequences, such as massive data leakage, the organisation or individual carrying out data processing activities will be fined not less than RMB 500,000 but not more than RMB 2 million, and may be ordered to suspend the relevant business or stop the business for rectification. Meanwhile, the persons directly in charge and other directly liable persons will be fined not less than RMB 500,000 but not more than RMB 2 million.

17 Enforcement and Sanctions

17.1 Describe the enforcement powers of the data protection authority(ies).

- (a) **Investigative powers:** The CAC, other relevant national departments (such as the MIIT, MPS and the SAMR), and relevant departments of local people's governments at or above the county level will respectively accept and handle complaints and reports related to data protection and may investigate illegal data processing activities.
- (b) **Corrective powers:** According to the PIPL, CSL and DSL, the CAC and relevant data protection authorities may issue an order warning to a make correction. For an entity who refuses to follow the instructions, it constitutes a non-compliance and incurs subsequent sanctions.
- (c) **Authorisation and advisory powers:** Relevant data protection authorities may guide personal information handlers to protect personal information by publishing national standards and other guidelines. For example, under Article 38 of the PIPL and the CBDT Assessment Measures, where a personal information handler needs to transfer information outside of China, it shall pass the security evaluation conducted by the CAC if they meet certain threshold requirements.
- (d) **Imposition of administrative fines for infringements of specified legal provisions:** The CAC and other

competent national departments (such as the MIIT, the MPS and the SAMR) are entitled to impose administrative fines on enterprises and the direct liable persons in violation of relevant data protection laws such as the DSL and PIPL.

- (e) **Non-compliance with a data protection authority:** According to the PIPL, CSL and DSL, the CAC and relevant data protection authorities may impose a fine, confiscate illegal gains, suspend any related business or shut down the business for rectification, and revoke any related business permit or its business licence as non-compliance sanctions.

17.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

Yes, and no court order is needed. For example, pursuant to Article 50 of the CSL, if any information prohibited by laws and administrative regulations from release or transmission is found, the CAC and other competent authorities may require the network operator to stop the transmission of such information, take measures such as deletion and keep the records. If any such information is from overseas, they may block the transmission.

17.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

The CAC and relevant data protection authorities may issue a ban in the form of an administrative penalty, together with other punitive measures such as a fine, an order to rectify, etc. In the recent special rectification action on app providers, the CAC, MIIT and its local branches usually issue a list of app providers and describe their illegal processing of personal information (such as excessive collection, lack of notification to users), and in cases where the app providers fail to make rectifications, the CAC, MIIT and relevant authorities may even request the apps to be removed from app stores.

17.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

So far, there is no public record of Chinese data protection authorities exercising their powers directly against companies established in other jurisdictions. In most cases, authorities may talk with the local subsidiary of an international company for its violations of the CSL or other data protection regulations.

18 E-discovery/Disclosure to Foreign Law Enforcement Agencies

18.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

In principle, China has always advocated the disclosure of data to foreign law enforcement agencies through judicial assistance approval of relevant authorities.

As for international judicial activities, under Article 4 of the International Criminal Judicial Assistance Law, it

provides that without the consent of the competent authorities of China, organisations and individuals within the territory of China shall not provide evidence materials to overseas entities.

As for specific personal information/data protection laws, both the PIPL and DSL prohibit handlers of personal information/data from providing personal information/data to foreign judicial or law enforcement authorities without the approval of competent authorities. If there are treaties or agreements in relation to judicial assistance or cooperation entered into between China and the respective foreign country, the relevant companies may respond to such requests following such treaties or agreements. Any entity or responsible person in violation of such requirement may be subject to administrative penalties. Furthermore, the Ministry of Justice published the Answers to Frequently Asked Questions on International Civil and Commercial Judicial Assistance, which specifically provides that where foreign judicial organisations or judicial personnel collect evidence materials located in China, they should first ask the Ministry of Justice for investigation.

In addition, there are also restrictions on foreign administrative agencies accessing data stored in China in certain industries. For example, Article 177 of the Securities Law requires that overseas securities regulatory authorities shall not carry out investigation and evidence collection, etc., directly within the territory of China. Moreover, without the approval of the securities regulatory authorities of the State Council and the relevant State Council departments, no organisations or individuals may provide the documents and materials relating to securities business activities to overseas parties arbitrarily. Also, Article 4 of the Counterespionage Law identifies acts such as the unauthorised provision of data concerned with national security and benefit to overseas authorities as espionage.

18.2 What guidance has/have the data protection authority(ies) issued on disclosure of personal data to foreign law enforcement or governmental bodies?

The CAC has not issued any guidance particularly concerning e-discovery requests from foreign law enforcement agencies in 2024.

19 Artificial Intelligence

19.1 Are there any limitations on automated decision-making involving the processing of personal data using artificial intelligence?

Automated decision-making using personal information shall be subject to transparency requirements; processors are required to ensure the fairness and impartiality of the decision, and shall not give unreasonable differential treatment to individuals in terms of trading price or other trading conditions.

Where information feeds or commercial marketing to individuals is carried out by means of automated decision-making, options not specific to individuals' characteristics shall be provided simultaneously, or convenient opt-out channels shall be made available. Individuals whose interests are materially impacted by the automated decision are entitled to request the relevant service provider/processor to provide explanations and to refuse to be subjected to decisions solely by automated means.

There are also transparency requirements for automated decision-making. Users of Internet information services involving AI technology are also entitled to be informed of the provision of algorithm-recommended services in a conspicuous manner. Relevant service providers are required to appropriately publish the basic principles, purposes and main mechanics of algorithm-recommended services.

19.2 What guidance (if any) has/have the data protection authority(ies) issued in relation to the processing of personal data in connection with artificial intelligence?

China's AI-related personal information protection regulatory framework operates as an integrated system, combining overarching foundational laws with specialised sector-specific regulations. The framework comprises:

- General legislation applicable to all digital activities: the CSL; the DSL; the PIPL; and the Network Data Security Administrative Regulation.
- AI-specific regulations providing detailed implementation: the Measure for the Management of Generative Artificial Intelligence Services; the CAC Algorithm Recommendation Rules; and the CAC Deep Synthesis Rules.

On 1 March 2024, after nearly six months of development, the Basic Security Requirements for Generative AI Services was officially released. The Basic Security Requirements for Generative AI Services provide detailed implementation rules for compliance requirements outlined in the Measure for the Management of Generative AI Services, such as lawful data sources and content security. It also offers practical guidance for generative AI service providers to conduct security assessments. The Basic Security Requirements for Generative AI Services not only help enterprises enhance their security capabilities for generative AI services, but also establish reference standards for regulatory authorities to evaluate the security levels of specific generative AI services.

20 Trends and Developments

20.1 In your opinion, what enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.

In 2024, the normalisation of cybersecurity enforcement has become increasingly evident, with regulatory authorities at all levels and regions continuing to intensify penalties for cybersecurity violations, particularly targeting sectors such as finance, information and communications, and local enterprises.

In terms of industry regulation, taking the financial sector as an example, the National Financial Regulatory Administration and its local offices have consistently issued administrative penalties related to information security violations by financial institutions. The identified breaches primarily involve the following issues: incomplete identification of critical information systems; inadequate disaster recovery preparedness and capabilities that fail to meet regulatory requirements; untimely remediation of system vulnerabilities, leading to potential risks; and deficiencies in information security management. The frequent issuance of penalties sends a strong signal that the financial sector, as a high-risk industry, must increase investment in cybersecurity and ensure compliance.

At the local enforcement level, cybersecurity authorities have also ramped up penalties against enterprises for failing to fulfil cybersecurity obligations. For instance, the cybersecurity division of the Inner Mongolia Public Security Bureau reported seven cases of non-compliance with cybersecurity protection duties, reinforcing the accountability of network operators. Administrative penalties were imposed on multiple violators for failing to establish proper management systems or fulfil cybersecurity obligations, including cases involving refusal to implement cybersecurity safeguards and the provision of vulnerable cybersecurity products with high-risk phishing flaws.

Meanwhile, the Shanghai Communications Administration established a dedicated task force, led by its Cybersecurity Management Department, to conduct a 2024 Cloud Service Security Special Governance Initiative. The inspection process included briefings, document reviews and Q&A sessions, focusing on areas such as corporate network operations, cloud service security policy implementation, risk management, platform monitoring, redundancy protection capabilities and emergency response drills. Identified issues in submitted materials were flagged for corrective action, further strengthening the foundation for stable and secure cloud service operations and enhancing overall enterprise cybersecurity resilience.

20.2 In your opinion, what “hot topics” are currently a focus for the data protection regulator?

- 1) AI has now emerged as a pivotal driver of the latest technological and industrial revolution, prompting China, the European Union, the United States and others to prioritise AI legislation. China has included AI legislation in the legislative agendas of both the 13th and 14th NPC Standing Committees, with the State Council listing the draft AI Law in its annual legislative plans for both 2023 and 2024. In 2024, China actively advanced precision legislative efforts in the fields of algorithms and AI. Relevant

national standards have proposed detailed regulatory requirements covering generative AI security assessments, training data compliance, data annotation and emergency management, with drafts released for public consultation.

We interpret these developments as indicative of steady progress in China’s AI legislation. The “sector-specific regulation + general legislation” model may become the dominant approach to AI governance, with the AI Law and industry-specific AI regulations jointly shaping China’s distinctive framework for AI governance.

- 2) The DSL anchors its framework on “important data” and imposes extended data security protection obligations on related processing activities. Since its enactment, sector-specific regulations on important data security management have been successively introduced in industries such as automotive, finance, and industrial and information technology. Meanwhile, the Network Data Security Management Regulations – a key administrative statute in this field – have further refined the identification criteria for important data and clarified the obligations of important data processors.

As the saying goes: “The vitality and authority of law lie in its enforcement.” We anticipate that in 2025, practical governance measures for important data (e.g., mechanisms for submitting risk assessment reports) will be progressively implemented. Enterprises that may process important data in their daily operations must legally comply with identification and reporting obligations. Furthermore, such important data processors, as well as network data processors potentially handling personal information of over 10 million individuals, should systematically fulfil their applicable obligations under sectoral legislation and the Network Data Security Management Regulations. This includes: refining internal mechanisms for identifying important data; establishing risk assessment procedures for data processing; and designating a data security officer and setting up a dedicated management body for network data security.



Susan Ning is a senior partner and the head of the Commercial and Regulatory Group. She is one of the pioneers engaged in the cybersecurity and data compliance practice, with publications in a number of journals such as the *Journal of Cyber Affairs*. Her articles include “New Trends of the US Personal Data Protection – Key Points of the New FCC Rules”, “Big Data: Success Comes Down to Solid Compliance”, “Does Your Data Need a “VISA” to Travel Abroad?”, and “A Brief Analysis on the Impact of Data on Competition in the Big Data Era”, among others. Susan was recognised as a “Tier 1 Lawyer” for Cybersecurity and Data Compliance in 2023 in *LEGALBAND China*.

Susan’s practice areas cover self-assessment of network security, responding to network security checks initiated by authorities, data compliance training, due diligence of data transactions or exchanges, compliance of cross-border data transmissions, etc. Susan has assisted companies in sectors such as IT, transportation, online payments, consumer goods, finance, Internet of Vehicles in dealing with network security and data compliance issues.

King & Wood Mallesons

18th Floor, East Tower, World Financial Centre
No.1 Dongsanhuan Zhonglu, Chaoyang District
Beijing 100020
China

Tel: +86 10 5878 5010
Email: susan.ning@cn.kwm.com
LinkedIn: www.linkedin.com/in/susan-ning-b901ab135



Han Wu practises in the areas of cybersecurity, data compliance and antitrust. He excels in providing cybersecurity and data compliance advice to branches of multinational companies in China from the perspective of data compliance in China. Han also has expertise in establishing network security and data compliance systems for Chinese enterprises going abroad in line with the requirements of the European Union (GDPR), the US and other cross-jurisdictions. Han was elected as one of “40-under-40 Data Lawyers” by *Global Data Review* in 2018. Han was also recognised as a “Next Generation Partner” by *The Legal 500* in 2021 and named one of the 2021 *ALB China* Top 15 TMT Lawyers. Additionally, in 2024, he was named by *Chambers* as a Leading Lawyer in Data Protection and Privacy in the TMT category. In the areas of cybersecurity and data compliance, Han provides legal services including: assisting clients to establish a cybersecurity compliance system; assisting clients in self-investigation on cybersecurity and data protection; assisting clients to conduct internal training on cybersecurity and data compliance; assisting clients in due diligence in data transactions; assisting clients to design plans for cross-border data transfers; and assisting clients in network security investigations and cybersecurity incidents, among others.

King & Wood Mallesons

18th Floor, East Tower, World Financial Centre
No.1 Dongsanhuan Zhonglu, Chaoyang District
Beijing 100020
China

Tel: +86 10 5878 5749
Email: wuhan@cn.kwm.com
URL: www.kwm.com/jp/en/people/wu-han.html

King & Wood Mallesons is an international law firm headquartered in Asia that advises Chinese and overseas clients on a full range of domestic and cross-border transactions, providing comprehensive legal services. Around the world, the firm has over 3,000 lawyers with an extensive global network of 31 international offices spanning Singapore, Japan, the US, Australia, the UK, Germany, Spain, Italy and other key cities in Europe, as well as presence in the Middle East. With a large legal talent pool equipped with local in-depth and legal practice, it provides legal services in multiple languages. King & Wood Mallesons, with its strong foundation and ever-progressive practice capacity, has been a leader in the industry. It has received more than 300 international and regional awards from internationally authoritative legal rating agencies, businesses and legal media, including *Acritas*, *The Financial Times*, *ALB*, *Who’s Who Legal*, *Chambers Asia-Pacific Awards*, *Euromoney*, *LEGALBAND*, *Legal Business*, *The Lawyer*, etc.

www.kwm.com

金杜律师事务所
KING & WOOD
MALLESONS

Egypt

Shehata & Partners



Ibrahim
Shehata



Tasneem
ElNaggar



Safa
Rabea

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The Personal Data Protection Law No. 151/2020 (“**PDPL**”) serves as the principal legislation for data protection in Egypt, focusing on safeguarding the privacy and data rights of individuals and entities. It mandates that organisations must obtain explicit consent from Data Subjects before processing their personal data and grants individuals various rights, including the ability to access, correct, erase or withdraw consent regarding their data and informing them in the case of any data violation. Additionally, the PDPL establishes clear principles for data processing, including fairness, transparency and minimisation, while imposing penalties for non-compliance, thereby reinforcing the importance of adhering to data protection standards.¹

1.2 Is there any other general legislation that impacts data protection?

Egypt’s data protection framework is influenced by several pieces of general legislation that provide legal safeguards for individual privacy and data security:

1. Constitutional Protection of Privacy

Privacy is a fundamental right enshrined in the 2014 Egyptian Constitution, which provides comprehensive legal protection for individuals. Article 57 explicitly states that “private life is inviolable, safeguarded, and may not be infringed upon”, ensuring protection against unlawful searches, seizures and bodily harm, as well as unauthorised entry, surveillance or interference in family relationships. The Constitution also guarantees the confidentiality of personal communications, including letters, emails, phone calls and electronic correspondence, prohibiting unauthorised collection, use or disclosure of personal data. Additionally, Article 57 reinforces the inviolability of communication channels – telegraph, postal, electronic and telephone – safeguarding them from interception or unlawful access. These constitutional provisions establish a strong foundation for data protection and privacy rights in Egypt.

2. Telecommunications Data Protection

The Telecommunications Law No. 10/2003 (“**Telecommunications Law**”) plays a crucial role in strengthening privacy protections, particularly in the

telecommunications sector. As advanced technologies continue to evolve, they rely on extensive data collection, making robust privacy safeguards essential. While the PDPL provides a broad regulatory framework for personal data security, the Telecommunications Law introduces additional sector-specific protections. It requires licensed operators to maintain the confidentiality of private communications and calls, establishing clear regulations to enforce these protections.² By complementing the PDPL, this law ensures enhanced privacy measures tailored to the unique challenges posed by telecommunications and emerging digital technologies.

Additionally, Decree No. 667/2017, issued by the Minister of Telecommunications and Information Technology establishes penalties for telecommunications service providers that violate regulations set by the National Telecommunication Regulatory Authority (“**NTRA**”) regarding user rights protection. It also enforces penalties for non-compliance with data privacy obligations outlined in service provider licences, reinforcing accountability and ensuring the protection of user data within the telecommunications sector.

3. Cybercrime Regulations

The Cybercrimes Law No. 175/2018 (“**Cybercrimes Law**”) and its executive regulation establish data privacy safeguards by regulating online activities and penalising unauthorised access to personal data and IT systems. Service providers are mandated to store user data for 180 days, maintain its confidentiality, and refrain from disclosing it without a judicial order. Additionally, they must implement security measures, such as encryption and multi-factor authentication, to prevent cyber threats and protect user data integrity.³ These requirements reinforce data privacy protections and align with broader cybersecurity regulations in Egypt.

4. E-Signature and IT Security

Law No. 15/2004, which regulates e-signatures and establishes the Information Technology Industry Development Agency and its executive regulations, mandates that electronic signature data, electronic media and information submitted to the licensed certification authority are considered confidential. Those who access or handle such information as part of their work are prohibited from disclosing it to third parties or using it for any purpose other than the one for which it was provided.⁴ Additionally, the Executive Regulations of this law require applicants for e-signature services to implement systems that ensure the security and confidentiality of information, aligning with legal standards.⁵

5. Criminal Law Protections

Law No. 58/1937 (“**Penal Code**”), as amended, criminalises the invasion of privacy and the unauthorised collection, use, or disclosure of personal information. It imposes penalties on individuals or entities that unlawfully access, obtain, or share personal data without legal justification, reinforcing data privacy protections under Egyptian law.⁶

1.3 Is there any sector-specific legislation that impacts data protection?

While the PDPL provides a comprehensive legal framework for safeguarding personal information, the Telecommunications Law introduces sector-specific regulations to further enhance privacy protections.

This law mandates licensed telecommunications operators to ensure the confidentiality of customer communications and private calls, preventing unauthorised access, interception, or disclosure.⁷

Furthermore, the Telecommunications Law stipulates that the NTRA is responsible for collecting, managing and updating the database of frequency spectrum users, with a strict obligation to maintain the confidentiality of this data to protect users’ right to privacy.⁸

By complementing the PDPL, the Telecommunications Law addresses the unique risks associated with the telecom industry, reinforcing privacy safeguards against emerging challenges such as cyber threats, mass data collection and technological advancements like AI and IoT. This sector-specific approach ensures that telecommunications service providers implement robust data security measures, maintaining trust and compliance within Egypt’s regulatory framework.

1.4 What authority(ies) are responsible for data protection?

Article 19 of the PDPL establishes the Data Protection Centre (“**PDPC**”) as the key regulator for data privacy and protection. The PDPC’s responsibilities include, *inter alia*:

- Setting policies and implementing procedures for personal data protection.
- Unifying data protection and processing policies.
- Coordinating with authorities to ensure data protection measures.
- Issuing licences and approvals related to data protection.
- Handling complaints and making necessary decisions.

Additionally, the PDPL’s 13th and 14th chapters grant PDPC employees’ judicial authority and outline penalties for violations, including reconciliation methods.⁹

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

The PDPL provides several foundational definitions that shape its scope and application. The following are the key terms for understanding the obligations, rights and regulatory framework established therein:¹⁰

- **“Personal Data”**
Any data related to an identified or identifiable natural person, either directly or indirectly, through linking

such personal data with any other data, such as name, voice, image, identification number, online identifier, or any data that determines the psychological, medical, economic, cultural or social identity of a natural person.

- **“Sensitive Personal Data”**
Data that discloses mental, psychological, physical or genetic health, biometric data, financial data, religious beliefs, political opinions or criminal status. In all cases, children’s data is considered sensitive personal data.
- **“Data Subject”**
Any natural person to whom personal data processed electronically pertains, either legally or practically, and who can be identified or distinguished from others.
- **“Processing”**
Any electronic or technical process for writing, collecting, recording, storing, preserving, merging, displaying, sending, receiving, circulating, publishing, erasing, altering, modifying, retrieving or analysing personal data using any medium, device or electronic or technical means, whether performed partially or entirely.
- **“Holder”**
Any natural or legal person who lawfully or effectively holds and retains personal data in any form, or on any storage medium, whether they are the originator of the data or have obtained possession of it in any manner.
- **“Controller”**
Any natural or legal person who, by virtue of the nature of their work, has the right to obtain personal data, determine the method, manner and criteria for its retention, processing and control, in accordance with the specified purpose or their activity.
- **“Processor”**
Any natural or legal person specialised by the nature of their work in processing personal data for their own benefit or on behalf of the Controller, in accordance with an agreement and their instructions.
- **“Disclosure of Personal Data”**
Any means that enables a third party to gain access to personal data, such as viewing, circulating, publishing, transferring, using, displaying, transmitting, receiving or disclosing it.
- **“Data Breach and Violation”**
Any unauthorised access to personal data or unlawful access to it, or any illegal process of copying, sending, distributing, exchanging, transferring or circulating aimed at revealing or disclosing personal data, or destroying, modifying or altering it during its storage, transmission or processing.
- **“Electronic Marketing”**
The sending of any message, statement, or advertising or marketing content through any technological means, regardless of its nature or form, aimed directly or indirectly at promoting goods or services, or solicitations or requests for commercial, political, social or charitable purposes, directed at specific individuals.

3 Territorial and Material Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The PDPL has extra-territorial effect and may apply to businesses established outside Egypt under certain circumstances.

Pursuant to Article 2 of the Issuance Law, the provisions of the PDPL apply in the following scenarios:

- If the offender is an Egyptian national, regardless of whether the offence occurs inside or outside Egypt.
- If the offender is a non-Egyptian residing in Egypt.
- If the offender is a non-Egyptian located outside Egypt, provided that:
 - a. the act is punishable under the laws of the country in which it occurred; and
 - b. the personal data subject to the offence relates to Egyptians or foreign residents within the Arab Republic of Egypt.

Accordingly, a business established in another jurisdiction may be subject to the PDPL if it processes personal data related to individuals residing in Egypt and the underlying activity constitutes an offence under both Egyptian law and the law of the country where the activity took place.¹¹

3.2 Do the data protection laws in your jurisdiction carve out certain processing activities from their material scope?

Article 3 of the Issuance Law of the PDPL outlines exceptions to its scope, excluding certain data processing activities, including:

- Data processed by a person for personal use.
- Data processed for media purposes, as long as it is truthful, accurate and complies with media laws.
- Data processed for official statistical purposes.
- Data related to legal investigations, inquiries and court proceedings.
- Data held by national security authorities.
- Data held by the Central Bank of Egypt and its supervised entities, except for money transfer and currency exchange companies.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

The PDPL sets out several core principles that govern the lawful and responsible processing of personal data. These principles primarily include:

- **Transparency**
The PDPL application of the principle of transparency lies at the heart of granting the Data Subject the right to know, review, access or obtain their own personal data that is in possession of any data Holder, Processor or Controller.¹² The PDPL also stipulates that the processing of personal data shall be for legitimate, specific and declared purposes related to the Data Subject.¹³ In addition, it obligates the data Processor to ensure the legitimacy of the purpose of the processing and its practice, as well as compliance with the public order or morals.¹⁴
- **Lawful basis for processing**
The PDPL states that processing is considered legitimate and legal when it satisfies one of the following conditions:
 - it is carried out upon the Data Subject's consent for achieving certain purposes;
 - it is necessary and intrinsic for performing contractual obligation or legal action, in executing an agreement for the benefit of the Data Subject, or in undertaking any procedures with respect to claiming or defending the Data Subject's legal rights;

- it is necessary for complying with legal obligations, orders issued by the competent investigation authorities or based on a judicial ruling; or
- it is necessary for the Controller to be able to perform its obligations or any relevant person to practice its legitimate rights; however, such performance does not contradict with the Data Subject's fundamental rights and freedom.¹⁵

- **Purpose limitation**

The PDPL regulates the processing of personal data through the principle of purpose limitation by requiring that any processing carried out by a data Processor or Controller shall be for legitimate, specific and declared purposes only.¹⁶

- **Data minimisation**

In line with the purpose limitation principle, the PDPL enforces data minimisation by requiring that only the minimum necessary personal data be collected and retained. Data Controllers and Processors are obligated to delete personal data once the intended purposes for its collection have been fulfilled.¹⁷

- **Proportionality**

The PDPL incorporates the principle of proportionality by requiring that any processing of personal data must be appropriate and not excessive in relation to the purposes for which it is collected. This means that data Controllers and Processors must ensure that the scope, volume and impact of data processing are proportionate to the intended and declared purpose.

- **Accuracy**

The principle of accuracy under the PDPL is reflected in the obligations imposed on the data Controller to ensure that personal data is valid, sufficient and consistent with the purpose for which it was collected. It also requires the data Controller to correct any errors in the personal data immediately upon becoming aware of them or being notified.¹⁸ Additionally, the PDPL grants the Data Subject the right to edit, delete, add to and update their personal data to ensure that it remains accurate and up to date.¹⁹ The PDPL further enforces the principle of accuracy by granting the PDPC the power to follow-up with the registration and updating of personal data records maintained by the data Controller or the processing activities' records maintained by the Processor, to ensure the accuracy of the data and information recorded therein.²⁰

- **Retention**

Retention is one of the core principles under the PDPL, and it is governed by several key provisions, including:

- a. The obligation that, in order for the data Controller or Processor to retain personal data, they must first ensure: (i) the legitimacy of the collection of such data for a specific and declared purpose to the Data Subject; (ii) the accuracy and security of the data; and (iii) that the retention period does not exceed what is necessary to fulfil the intended purpose.²¹
- b. The obligation to delete any personal data in the Controller's possession once the designated purpose has been fulfilled. However, if the personal data is retained for a legitimate reason after the satisfaction of its purpose, such data shall be retained in an anonymised form.²²
- c. The obligation to delete personal data upon the expiration of the processing period applicable to the data Processor.²³

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

Under the PDPL, Data Subjects are granted specific rights, complemented by general obligations imposed on both data Controllers and Processors to safeguard those rights. These rights include:²⁴

- **Right of access to (copies of) data/information about processing**
The PDPL grants Data Subjects the right to be informed of the personal data held about them by any Controller or Processor. This includes the right to access and obtain a copy of their data, as well as information regarding the nature, purpose and scope of its processing.
- **Right to rectification of errors**
Data Subjects have the right to request the correction, amendment, updating or completion of inaccurate or incomplete personal data held by Controllers or Processors.
- **Right to deletion/right to be forgotten**
The PDPL entitles Data Subjects to request the deletion of their personal data. Additionally, data Controllers and Processors are required to delete the personal data collected upon the completion of the initial purpose in which the personal data was collected.
- **Right to object to processing**
The PDPL grants Data Subjects the right to object to the collection, processing, disclosure or dissemination of their personal data without their explicit consent, except where such processing is authorised by law.
- **Right to restrict processing**
A Data Subject has the right to restrict the processing within a defined scope and purpose.
- **Right to data portability**
The PDPL grants various rights to Data Subjects; however, these rights do not expressly include the right to data portability.
- **Right to withdraw consent**
The PDPL grants the right to withdraw consent for the retention or processing of their personal data at any time. Upon withdrawal, the data Controller or Processor must cease all processing activities related to that data, unless a legal obligation or overriding legitimate interest justifies continued processing.
- **Right to object to marketing**
The PDPL prohibits any electronic communication for the purpose of direct marketing to the Data Subject, without acquiring their consent for such purpose.²⁵
- **Right protecting against solely automated decision-making and profiling**
The PDPL grants the right to object to the processing of personal data if it conflicts with the Data Subject's fundamental rights and freedoms. Accordingly, if Automated Decision-Making ("ADM") or profiling poses such a conflict, the Data Subject may exercise the right to object to that processing.
- **Right to complain to the relevant data protection authority(ies)**
Without prejudice to the right to seek judicial remedies, the PDPL grants Data Subjects and any party with a legitimate and direct interest the right to lodge a complaint with the PDPC in the following cases: (i) violation or infringement of personal data protection rights;

(ii) failure to enable the Data Subject to exercise their rights; or (iii) objections to decisions issued by the Data Protection Officer ("DPO") of the Controller or Processor regarding submitted requests.²⁶

- **Right to compensation**

The PDPL imposes a range of criminal and administrative penalties for violations of personal data protection obligations. Fines range from EGP 100,000 to EGP 5 million, and in certain cases, imprisonment of not less than three to six months may also apply – particularly for unlawful processing of sensitive personal data or cross-border data transfers in breach of the law. Offences include unauthorised data collection, disclosure or processing, failure to enable Data Subject rights, non-compliance with licensing or security obligations, and breaches by DPOs or legal representatives. In cases of repeated offences, penalties are doubled. Additionally, courts may order the publication of convictions in widely circulated newspapers and online platforms at the offender's expense, and attempt (incomplete crimes) is punishable by half the prescribed penalty. Legal representatives and corporate entities may also be held jointly liable for damages resulting from violations committed in their name or for their benefit.²⁷

5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

Egyptian law does not include a dedicated legal framework or specific legislation for collective redress, such as class action lawsuits, as seen in some other jurisdictions like the EU with the Representative Actions Directive. However, there are procedural avenues through which individuals with similar claims can collectively seek redress, including in cases involving violations of personal data:

- **Representation by Associations or Legal Entities:** Organisations such as consumer protection associations, labour unions or NGOs can represent groups of individuals in disputes. For example, employees whose personal data has been mishandled by an employer or a labour entity can collectively seek redress with the support of a union. Similarly, NGOs advocating for data privacy rights can assist individuals in pursuing claims related to data breaches or misuse by companies.
- **Consumer Protection Authority:** Under the Consumer Protection Law, the Consumer Protection Authority is empowered to file lawsuits on behalf of consumers harmed by widespread violations, including cases of unlawful data collection, misuse or insufficient safeguards for personal data. This provides a practical avenue for consumers affected by systemic data protection violations to pursue remedies collectively.²⁸

6 Children's Personal Data

6.1 What additional obligations apply to the processing of children's personal data?

The PDPL classifies children's data as sensitive personal data, in which it requires heightened care in handling. In this respect, the PDPL mandates Processors to obtain explicit consent from the child's legal guardian before collecting or processing any data. Additionally, the PDPL stipulates that the

processing of children's data must be limited to specific, legitimate purposes, and only the minimum necessary data should be collected for such purposes.

Furthermore, the PDPL prohibits the collecting, processing, handling, disclosing, saving, retaining and transferring of sensitive personal data except by virtue of a licence obtained from the PDPC.²⁹

7 Registration Formalities and Prior Approval

7.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

Under the PDPL, businesses engaged in the processing of personal data are legally required to obtain a licence or permit from the PDPC prior to commencing processing activities. This applies to data Controllers, data Processors and entities engaged in sensitive personal data or cross-border data transfers involving personal data.³⁰

The PDPL further requires that businesses maintain internal records of processing operations, assign a DPO, and cooperate with inspections and oversight by the PDPC.

Failure to obtain the appropriate authorisation or comply with registration obligations may result in administrative fines or criminal penalties.

7.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

Under the PDPL, the registration and licensing framework is designed to be specific and structured, rather than general. Articles 26 and 27 make clear that the PDPC is responsible for issuing various types of licences, permits and accreditations based on the nature of the processing activity. These include authorisations for data retention and processing, direct electronic marketing, processing of sensitive personal data, visual surveillance and cross-border data transfers, among others.

While the executive regulations of the PDPL are yet to be issued, they are expected to define the categories, procedures, conditions, levels and forms associated with each type of licence or permit. Based on the PDPL, it is anticipated that registration will require granular information rather than high-level or generic descriptions of data processing activities.

Therefore, until the executive regulations are published, businesses should prepare to meet specific and comprehensive disclosure requirements as part of the licensing process, aligned with the PDPC's templates and evaluation criteria.

7.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

Under Article 27 of the PDPL, applications for licences, permits or accreditations must be submitted to the PDPC using the official forms it issues, along with the required documents and evidence of financial and technical capacity.

The PDPL expressly allows for multiple licences or permits to be issued to a single Controller or Processor, depending on

the type of personal data being processed. Specifically, the law states:

"...the Controller or Processor may obtain more than one license or permit depending on the type of Personal Data being dealt with."

Therefore, the basis for registration under the PDPL may vary according to the nature or category of personal data. Further details regarding additional bases – such as legal entity, processing purpose or system – are expected to be specified in the forthcoming executive regulations.

7.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

While the PDPL does not explicitly state that these categories of entities must register or notify the PDPC, the licensing requirements under the PDPL apply to all data Controllers and Processors seeking to process personal data. This includes:

- Processors/Controllers operating within Egypt;
- foreign data Controllers and Processors that process personal data of individuals located in Egypt; and
- branches of foreign legal entities operating in Egypt that process personal data of individuals located in Egypt.

Therefore, any entity – whether domestic or foreign – that processes personal data of individuals within Egypt or conducts regulated data processing activities must comply with the PDPL's registration and licensing obligations, in accordance with Articles 26 and 27 of the PDPL. Further procedural details are expected to be clarified in the forthcoming executive regulations.

7.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

The PDPL requires that applications for licences, permits or accreditations be submitted to the PDPC using official forms prepared by it. According to Article 27, each application must be accompanied by:

- all documents and information as specified by the PDPC;
- evidence of the applicant's financial capability; and
- proof of the applicant's ability to meet and implement the prescribed technical requirements and standards.

Additionally, the PDPC is authorised to:

- request any additional documents, data or guarantees it deems necessary to assess the adequacy of personal data protection; and
- require supplementary safeguards if the measures described in the application are considered insufficient.

While the specific categories of required information – such as types of personal data, categories of Data Subjects, and processing purposes – are not explicitly listed in the law, Article 26(1) clarifies that the executive regulations will determine the detailed procedures, conditions and templates to be used for such submissions.

7.6 What are the sanctions for failure to register/notify where required?

Failure to obtain the required licences, permits or

accreditations from the PDPC prior to conducting personal data processing activities is subject to penal sanctions under the PDPL. Specifically, Article 45 provides that:

“A fine of no less than EGP 500,000 and not exceeding EGP 5,000,000 shall be imposed on any person who violates the provisions governing licensing, permits, or accreditations as stipulated under this Law.”

This penalty applies to any Controller or Processor that processes personal data without the appropriate authorisation required under Articles 26 and 27, which govern the classification, issuance and procedural requirements for such licences and permits.

7.7 What is the fee per registration/notification (if applicable)?

According to Article 26 of the PDPL, the PDPC is authorised to charge fees for the issuance of licences, permits and accreditations. The maximum fees are as follows:

- Up to EGP 2 million for a licence.
- Up to EGP 500,000 for a permit or accreditation.

The exact fee amounts, categories and payment procedures will be determined in the executive regulations, which are yet to be issued.

7.8 How frequently must registrations/notifications be renewed (if applicable)?

The PDPL provides that the renewal procedures, durations and conditions for licences, permits and accreditations will be specified in the executive regulations.³¹

As of now, the PDPL does not stipulate a specific renewal frequency. Entities subject to the law will be required to comply with the timelines and procedures set out in the executive regulations once issued.

7.9 Is any prior approval required from the data protection regulator?

The PDPL requires prior approval from the PDPC before carrying out certain personal data processing activities. Under Article 26, Controllers and Processors must obtain licences or permits for:

- data retention, processing and handling activities;
- cross-border transfers of personal data;
- direct electronic marketing;
- processing of sensitive personal data;
- use of visual surveillance tools in public spaces; and
- processing carried out by associations, unions or clubs concerning their members' data.

The PDPC evaluates licence or permit applications in accordance with the procedures outlined in Article 27 and may require additional guarantees or supporting documents. No processing may lawfully commence before the relevant licence or permit is granted.

7.10 Can the registration/notification be completed online?

The PDPL does not explicitly specify whether registration, licensing or notification procedures can be completed online.

However, the executive regulations, once issued, are expected to detail the submission methods, including whether

an online application platform will be available. Until such regulations are in force, the availability of online registration remains unconfirmed.

7.11 Is there a publicly available list of completed registrations/notifications?

The PDPL does not currently provide for the publication of a publicly accessible list of completed registrations, licences or notifications.

The matter of public access to registration information may be addressed in the forthcoming executive regulations, which are expected to define procedural and transparency requirements in more detail.

7.12 How long does a typical registration/notification process take?

The process of acquiring a licence, permit or certificate shall not exceed 90 days from the day of the completion of all information and documentation; the lapse of this specified period shall be deemed as rejection of the application.³²

8 Appointment of a Data Protection Officer

8.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

Under the PDPL, the appointment of a DPO is mandatory for all legal entities acting as data Controllers or Processors. Article 8 requires the legal representative of such entities to appoint a competent employee responsible for personal data protection, register them with the PDPC and publicly announce the appointment.

For natural persons acting as Controllers or Processors, they are personally responsible for complying with the law's provisions.

The PDPL does not provide exemptions based on the size of the organisation or the volume of data processed; hence, the DPO requirement applies universally to all legal entities processing personal data.

8.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

The PDPL stipulates that organisations that fail to appoint a DPO shall be penalised with a fine not less than EGP 200,000 and not exceeding EGP 2 million as a non-compliance fine.³³

8.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

The PDPL does not provide employment protections for DPOs against disciplinary measures or adverse consequences related to the performance of their duties. However, the law does impose personal liability on DPOs who fail to fulfil their legal obligations.

According to Article 40, a DPO who fails to comply with their responsibilities may be subject to an administrative fine of not less than EGP 200,000 and not exceeding EGP 2 million. In cases where the violation results from negligence, the penalty ranges from EGP 50,000 to EGP 500,000.

8.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

Under the PDPL, each legal entity acting as a data Controller or Processor is required to appoint a DPO within its own organisational structure. Article 8 mandates that the legal representative of a juristic person must appoint a competent employee as a DPO, register them with the PDPC and publicly announce the appointment.

The law does not explicitly address whether a single DPO can serve multiple entities, such as across a corporate group. Therefore, until the executive regulations provide further clarification, it is advisable for each legal entity to appoint its own DPO to ensure compliance with the PDPL.

8.5 Please describe any specific qualifications for the Data Protection Officer required by law.

While the PDPL outlines the responsibilities of the DPO in Article 9, it does not specify particular qualifications or criteria for the role. The forthcoming executive regulations are expected to provide detailed requirements regarding the qualifications and competencies necessary for individuals appointed as DPOs.

8.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

Under Article 9 of the PDPL, the DPO is responsible for implementing the provisions of the law, its executive regulations and the decisions of the PDPC. The DPO is required to monitor and supervise internal data protection procedures and handle Data Subject requests.

Key responsibilities include:

1. Conducting regular assessments of data protection systems and documenting results.
2. Acting as the main point of contact with the PDPC and executing its decisions.
3. Enabling Data Subjects to exercise their legal rights.
4. Notifying the PDPC of any data breaches.
5. Responding to Data Subject inquiries and complaints.
6. Maintaining and updating the data register (Controller) or processing operations register (Processor).
7. Identifying and correcting data protection violations internally.
8. Organising training programmes for employees on data protection compliance.

Additional obligations may be detailed in the forthcoming executive regulations.

8.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

As per the PDPL, the appointment of a DPO must be registered with the PDPC. Article 8 mandates that the legal representative of any legal entity acting as a data Controller or Processor

appoint a competent employee as a DPO. This appointment must be registered in the official DPO register maintained by the PDPC, and the appointment must be publicly announced.

8.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

As per Article 8 of the PDPL, the appointment of a DPO shall be publicly announced. However, the law does not explicitly mandate that the DPO's name or contact details be included in a public-facing privacy notice or equivalent document.

Nonetheless, best practices suggest that organisations should provide clear contact information for their DPO in their privacy notices to facilitate communication with Data Subjects and demonstrate transparency in data processing activities.

9 Appointment of Processors

9.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

It is mandatory for a data Controller to enter into a written agreement with any Processor that processes personal data on its behalf. Article 5 of the PDPL stipulates that a Processor must conduct processing activities based on written instructions received from the Controller, the PDPC or any relevant authority.

Therefore, to ensure legal compliance and clarity in roles and responsibilities, businesses must establish comprehensive written agreements with their Processors when outsourcing personal data processing activities.

9.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

When a business appoints a Processor to process personal data on its behalf, the business is required to enter into a written agreement with the Processor. This agreement must clearly outline the Processor's obligations, including the purpose and scope of data processing, the security measures to be implemented, and the Processor's duty to comply with the law and protect individuals' privacy. The agreement should also specify that the Processor will only process the data in accordance with the business's instructions and ensure that the data is not used for any other purposes.³⁴

10 Marketing

10.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

Under Articles 17 and 18 of the PDPL, electronic direct marketing is subject to strict prior consent requirements and transparency obligations. Specifically:

- Consent requirement: Direct marketing communications via any technological means (including email, SMS or instant messaging) are prohibited without the explicit prior consent of the Data Subject.

- Mandatory disclosures in each message:
 1. The identity of the initiator and sender.
 2. A valid and reachable address for the sender.
 3. A clear indication that the message is for marketing purposes.
 4. Simple and accessible opt-out mechanisms allowing the Data Subject to withdraw consent at any time.
- Obligations on the sender:
 1. Limit communications to the specific marketing purpose consented to.
 2. Do not disclose the contact details of the recipient to third parties.
 3. Maintain electronic records of the Data Subject's consent and any modifications to it for a period of three years from the date of the last message.³⁵

10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

The PDPL does not explicitly distinguish between business-to-consumer (“B2C”) and business-to-business (“B2B”) contexts. The restrictions on electronic direct marketing under Articles 17 and 18 apply broadly to any processing of personal data, including contact information used for marketing purposes. Therefore, if a B2B marketing communication involves the use of identifiable personal data (e.g., a named employee's email or phone number), the same prior explicit consent requirements would apply.

10.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

The PDPL defines electronic marketing broadly as the sending of any advertising or promotional message via any technological means, whether direct or indirect, and regardless of its format, when targeted to specific individuals.³⁶

As such, the PDPL's consent and opt-out requirements apply to any form of technology-based marketing, including emails, SMS, messaging apps or automated calls. However, the PDPL does not explicitly regulate traditional marketing methods, such as postal mail or physical leaflets. Unless these methods fall under the definition of electronic marketing by involving a technological medium, they are currently not subject to the PDPL's consent and opt-out requirements.

10.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?

The PDPL applies to marketing communications originating outside Egypt if they involve the processing of personal data of individuals located in Egypt. As per Article 2 of the Issuance Law, the PDPL has extra-territorial effect when:

- the sender is a non-Egyptian;
- the Data Subject is an Egyptian or a foreign resident in Egypt; and
- the act (e.g., unsolicited electronic marketing) is punishable under the law of the country where it was committed.

Accordingly, direct marketing sent from abroad to individuals in Egypt is subject to the same consent and compliance obligations under Articles 17 and 18.

10.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

While the law grants the PDPC clear enforcement powers – such as investigation, inspection, issuing warnings and imposing fines – practical enforcement activity is expected to become more visible following the issuance of the executive regulations and the full operationalisation of the PDPC.

10.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Under the PDPL, purchasing marketing lists from third parties is not explicitly prohibited. However, any use of such lists for electronic direct marketing must comply with the PDPL's strict requirements, particularly those outlined in Articles 17 and 18.

10.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Under Article 43 of the PDPL, sending electronic marketing communications in breach of the restrictions set out in Articles 17 and 18 is punishable by an administrative fine of no less than EGP 200,000 and not exceeding EGP 2 million.

These penalties apply to violations such as:

- Sending marketing messages without prior consent.
- Failing to identify the sender or provide opt-out mechanisms.
- Disclosing contact data without authorisation.

11 Cookies

11.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

While specific cookie regulations are not explicitly legislated, cookie usage is governed by the broader frameworks of the PDPL and related privacy laws, as outlined in question 1.2. These laws set requirements for data collection and processing that apply to cookies when they involve personal data:

- **Consent:** Cookies that collect personal data require the user's explicit consent before deployment. This applies to cookies used for purposes beyond basic website functionality, such as analytics or marketing.
- **Transparency:** Users must be informed about the types of cookies used, their purpose and how their data will be processed, typically through a clear and accessible cookie policy.
- **Purpose Limitation:** Cookies must collect and process data only for legitimate, declared and specific purposes, and the data collected should not exceed what is necessary for these purposes.
- **Right to Opt-Out:** Users must be provided with a mechanism to manage or decline non-essential cookies. This ensures compliance with the PDPL's requirement for respecting Data Subject rights.
- **Retention and Deletion:** Data collected through cookies must be retained only for the duration necessary to achieve the intended purpose and deleted or anonymised thereafter.

- **Security Measures:** Website operators must implement technical and organisational measures to ensure the security of data collected through cookies, preventing unauthorised access or misuse.³⁷

11.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

The law does not explicitly distinguish between different types of cookies in its current text. However, since cookies involve the processing of personal data when they identify or track individuals, their use – particularly for profiling or marketing – would fall under the general PDPL rules governing consent and lawful processing.

11.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

As of now, the PDPC is not yet fully operational, and the executive regulations, which are expected to clarify technical enforcement areas such as cookies, have not yet been issued.

11.4 What are the maximum penalties for breaches of applicable cookie restrictions?

While the PDPL does not specifically reference cookies, the use of cookies that involve the processing of personal data without proper legal basis – such as without licensing – would be treated as a violation of the law's general data protection provisions.

Accordingly, under Article 45 of the PDPL, the maximum penalty for breaches related to unlicensed or unauthorised processing activities (which may include improper use of tracking technologies like cookies) is a fine of no less than EGP 500,000 and up to EGP 5 million.

Additional sanctions may apply depending on the nature of the violation and whether it overlaps with marketing or consent-related infractions addressed in other articles.

12 Restrictions on International Data Transfers

12.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Under Articles 14–16 of the PDPL, the transfer of personal data to jurisdictions outside Egypt is restricted and may only occur under specific conditions:

- **Adequate Protection:** The receiving country must have data protection standards equal to or higher than those required under the PDPL.
- **PDPC Authorisation:** The Controller or Processor must obtain a licence or permit from the PDPC before initiating the transfer.
- **Additional Safeguards:** The PDPC may require the implementing of further protective measures depending on the nature of the data or risk involved.³⁸

12.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

In accordance with Articles 14 and 15 of the PDPL, cross-border transfers of personal data generally require:

- that the destination country ensures adequate protection; and
- prior authorisation from the PDPC.

However, Article 15 allows for specific exceptions where the destination country lacks adequate protection, provided there is explicit consent from the Data Subject or their representative. These exceptions include:

1. to preserve the life, health or medical care of the Data Subject;
2. to establish, exercise or defend legal rights before judicial authorities;
3. to perform or conclude a contract between the Controller and a third party for the benefit of the Data Subject;
4. in connection with international judicial cooperation;
5. where there is a legal obligation or necessity to protect the public interest;
6. for financial transfers conducted in compliance with the receiving country's regulations; and
7. where the transfer is carried out under a bilateral or multilateral international agreement to which Egypt is a party.

12.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

Under Article 14 of the PDPL, cross-border transfers of personal data require prior approval (licence or permit) from the PDPC. Transfers requiring PDPC approval typically include personal data that is collected or prepared for processing and is intended to be transferred, stored or shared with a foreign country, particularly when it involves sensitive personal data or inadequate protection levels.

In order to apply for said licence or permit, an application must be submitted on the forms produced by the PDPC attaching all the necessary supporting materials, demonstrating the applicant's financial stability and the applicant's technical competence. Following the completion of all the applications, decisions must be made within a timeframe of no more than 90 days. The application will be declared rejected if the allotted time has passed without a decision from the relevant authority in the PDPC.³⁹

12.4 Do transfers of personal data to other jurisdictions require a transfer impact assessment? If conducting a transfer impact assessment is only mandatory in some circumstances, please identify those circumstances.

The PDPL does not explicitly mandate a transfer impact assessment as a standalone requirement. However, Article 27 authorises the PDPC to request supporting documents and

additional guarantees when evaluating applications for cross-border data transfer licences.

12.5 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?

The PDPL is a domestic framework and does not directly incorporate or reference EU law or jurisprudence. Nevertheless, the PDPL emphasises the importance of ensuring that cross-border data transfers meet adequate protection standards. The PDPC, upon its operation, may take international developments into account when stipulating its regulations and guidance on data transfers.

12.6 What guidance (if any) has/have the data protection authority(ies) issued in relation to the use of standard contractual/model clauses as a mechanism for international data transfers?

As of now, the PDPC has not issued any official guidance on the use of standard contractual clauses or model data transfer agreements as a lawful mechanism for cross-border transfers under the PDPL.

13 Whistle-blower Hotlines

13.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

Egypt lacks comprehensive laws and regulations on whistle-blowing. However, some companies define misconduct eligible for reporting, focusing on serious violations that could harm the organisation or its stakeholders. These may include providing whistleblower hotlines for reporting illegal or unethical conduct, such as violations of company policies, corruption, fraud, embezzlement, harassment and other misconduct that breaches the organisation's code of ethics or applicable laws.

13.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

The PDPL does not explicitly prohibit or regulate anonymous reporting. It also does not expressly permit or encourage it. Therefore, anonymous reporting is not prohibited under the law, but any processing of personal data resulting from such reports must still comply with the PDPL's general principles.

Businesses are encouraged to implement a comprehensive whistleblowing policy as part of their internal governance framework. This policy can establish clear procedures for reporting misconduct or unethical behaviour while protecting the anonymity and safeguarding whistleblowers from retaliation.

14 CCTV

14.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

Under the PDPL, means of visual surveillance in public places shall be subject to acquiring a licence. According to Article 26(5), the PDPC is responsible for issuing licences or permits for the use of visual monitoring tools in public spaces. This includes CCTV systems used by businesses, public entities or private operators where surveillance may capture identifiable individuals. In addition to the licensing requirement, the consent of the Data Subject is required when the surveillance results in the collection or processing of identifiable personal data, unless another legal basis under the PDPL applies.

14.2 Are there limits on the purposes for which CCTV data may be used?

The use of CCTV data is subject to the purpose limitation principle under the PDPL. This means that any personal data, including video surveillance footage, may only be processed for specific, legitimate and declared purposes.

While the PDPL does not list specific acceptable CCTV purposes, it imposes the following general limits:⁴⁰

- Surveillance data must not be used for any purpose that is incompatible with the reason it was originally collected (e.g., security or safety).
- The use of CCTV data must be lawful and must not violate public order or morality.

If the data is processed for any purpose beyond its original intent, this would require separate consent or a valid legal basis.

15 Employee Monitoring

15.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Employee monitoring is permitted under Egyptian law provided it complies with the PDPL, the Egyptian Constitution and the Labour Law. Permissible types of monitoring may include CCTV, access logs and system usage tracking, provided that:

- the monitoring is clearly linked to a legitimate business purpose, such as protecting company assets, preventing data leaks or ensuring compliance with internal policies;
- it is limited to company-owned systems and property; monitoring personal devices is discouraged due to constitutional privacy protections (Article 57);
- it does not involve private communications or areas unless backed by prior judicial authorisation; and
- it aligns with the employer's obligation to protect work documents and confidential information under Labour Law Articles 56–57 and related disciplinary regulations.

To mitigate risks, companies are advised to prohibit the use of personal devices for work-related activities and restrict monitoring to company-issued equipment only.

15.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Under Article 2 of the PDPL, prior explicit consent is required for collecting or processing personal data, including monitoring activities. In practice, employers typically obtain consent and provide notice through:

- employment contracts containing clauses on data processing and surveillance;
- internal policies and handbooks, which clearly outline the scope of monitoring and device use restrictions; and
- onboarding acknowledgments and policy sign-offs, ensuring employees are fully informed.

15.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

Egyptian law does not require employers to notify or consult works councils, trade unions or employee representatives specifically in relation to employee monitoring policies or systems, including data processing or surveillance mechanisms.

However, under the Labour Law, employers are generally encouraged to promote social dialogue and may choose to engage employee representatives on broader workplace matters.

15.4 Are employers entitled to process information on an employee's attendance in office (e.g., to monitor compliance with any internal return-to-office policies)?

Employers are permitted to process information relating to an employee's attendance in the workplace, including for the purpose of monitoring compliance with internal return-to-office policies, provided they comply with the PDPL and other applicable laws.

Key conditions are as follows:

- Lawful basis: Attendance tracking can be based on the employer's legitimate interest or as part of fulfilling a contractual obligation (e.g., working hours, productivity).
- Data minimisation: Only the data necessary for verifying presence or absence should be collected.
- Transparency: Employees must be informed, through policies, contracts or notices, about the data being collected and the purposes of use.
- Security: Measures must be in place to protect attendance data from unauthorised access or misuse.

If attendance tracking involves biometric data (e.g., fingerprint or facial recognition), then explicit consent and PDPC licensing may be required due to its classification as sensitive personal data under the PDPL.

16 Data Security and Data Breach

16.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

The PDPL mandates that data Controllers and Processors must adopt all necessary technical and regulatory measures to protect personal data. This includes ensuring confidentiality,

integrity and availability of personal data against unauthorised access, alteration or destruction.⁴¹

Furthermore, the PDPL stipulates that each Controller or Processor shall appoint a DPO, who will be responsible for overseeing compliance with data protection regulations and ensuring that security measures are effectively implemented.⁴²

16.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Under Article 7 of the PDPL, both Controllers and Processors must report any personal data breach or violation to the PDPC within 72 hours of becoming aware of it. If the breach relates to national security, the notification must be made immediately. The report must include the following:

- a description of the breach (nature, form, cause and approximate volume of affected data);
- the contact details of the DPO;
- potential consequences of the breach;
- actions taken and proposed to address the breach and limit its impact;
- documentation and corrective measures; and
- any additional information requested by the PDPC.

16.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

According to Article 7 of the PDPL, data Controllers and Processors are also required to notify affected Data Subjects of the breach within three working days from the date the breach was reported to the PDPC.

This obligation ensures that individuals are made aware of incidents affecting their personal data and are able to take steps to protect themselves. Further details regarding the form and method of notification shall be addressed in the forthcoming executive regulations.

16.4 What are the maximum penalties for personal data security breaches?

Under Article 38 of the PDPL, a personal data security breach resulting from a Controller or Processor's failure to meet their legal obligations, such as failing to protect, secure or properly handle personal data, may be subject to:

- An administrative fine of no less than EGP 300,000 and up to EGP 3 million.

Additional penalties may apply under other articles depending on the nature of the breach, including:

- Criminal penalties in cases involving intentional misconduct or serious harm.
- Increased sanctions for violations involving sensitive personal data, unauthorised cross-border transfers or non-compliance with PDPC orders.

17 Enforcement and Sanctions

17.1 Describe the enforcement powers of the data protection authority(ies).

The PDPC is vested with comprehensive enforcement, supervisory and advisory powers to ensure compliance with data protection obligations and safeguard the rights of Data Subjects. These powers include, *inter alia*:

- **Investigative powers:** The PDPC has the authority to investigate complaints filed by Data Subjects or other interested parties in cases of personal data rights violations, denial of access or objectionable decisions made by Controllers or Processors. It must issue a decision within 30 working days.⁴³
- **Corrective and supervisory powers:** The PDPC may issue warnings and require violators to remedy breaches within a specified timeframe. If non-compliance continues, it may suspend, revoke, or cancel licences or permits, subject the violator to technical supervision at their own expense, or publicly disclose the violation.⁴⁴
- **Authorisation and advisory powers:** The PDPC is empowered to grant, amend, suspend or revoke licences, permits and accreditations for data processing activities. It may also issue guidelines, technical standards, and best practice recommendations in line with national and international developments.⁴⁵
- **Judicial enforcement authority:** PDPC-designated officials, authorised by the Ministry of Justice, hold judicial enforcement powers to record and report legal breaches of the PDPL.⁴⁶
- **Non-compliance with a data protection authority:** Failure to comply with directives issued by the PDPC can lead to various consequences. The authority may publish details of non-compliance in the media, subject violators to technical supervision at their own expense and impose further penalties. Additionally, individuals or entities may face legal action for non-compliance.⁴⁷

17.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The PDPC does have the authority to restrict or regulate specific types of data processing activities at a national level, including issuing general bans or limitations where necessary to protect personal data.

While the law does not explicitly use the term “ban”, it empowers the PDPC to:⁴⁸

- issue binding decisions, regulations and standards for data protection;
- approve or reject licensing requests for specific processing activities;
- set conditions for sensitive data processing or cross-border transfers; and
- coordinate with national security authorities in cases involving public interest.

In effect, this enables the PDPC to prohibit certain categories of processing by refusing authorisations or setting regulatory restrictions.

17.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

The PDPC has not yet commenced active enforcement of the PDPL. However, once it is operational, the PDPC is expected to exercise its authority through a range of activities, including overseeing compliance with data protection regulations, providing guidance and clarification on the application of the law, and ensuring the protection of individuals’ personal data rights.

17.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

While the PDPL applies extraterritorially to businesses established outside Egypt that process the personal data of individuals located within Egypt, the PDPC cannot unilaterally enforce its powers over such entities.

In practice, for the PDPC to exercise or enforce its decisions outside Egypt against a foreign business, it may only do so through certain recognised legal channels, such as:

- obtaining a court judgment in Egypt and seeking its recognition and enforcement in the foreign country in accordance with that country’s laws on the enforcement of foreign judgments; or
- acting under the framework of a bilateral or multilateral treaty that enables cross-border enforcement cooperation in data protection matters.

Absent such channels, the PDPC’s decisions have no direct binding effect on entities outside Egypt’s jurisdiction, unless those entities have a presence or representative in Egypt or voluntarily comply.

18 E-discovery/Disclosure to Foreign Law Enforcement Agencies

18.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

The PDPL does not specify regulation in regard to requests for disclosure to foreign law enforcement agencies. However, businesses must ensure that any disclosure of data complies with the PDPL in terms of consent or legitimate justification, and the regulations regarding the provisions of cross-border data transfer.

18.2 What guidance has/have the data protection authority(ies) issued on disclosure of personal data to foreign law enforcement or governmental bodies?

As of now, the PDPC is not yet operational, and no formal guidance has been issued regarding the disclosure of personal data to foreign law enforcement or governmental bodies.

However, Article 25 of the PDPL provides a general legal basis for future cooperation. It empowers the PDPC, once active, to coordinate with foreign counterparts under international, regional or bilateral cooperation agreements, particularly where such cooperation supports:

- The protection of personal data and prevention of violations.

- Verification of compliance by Controllers or Processors outside Egypt.
- Information exchange to assist in investigations and trace offenders involved in data-related crimes.

19 Artificial Intelligence

19.1 Are there any limitations on automated decision-making involving the processing of personal data using artificial intelligence?

The PDPL does not contain explicit provisions regulating ADM or profiling using Artificial Intelligence (“AI”). However, the PDPL’s general data protection principles indirectly apply to such activities. Therefore, the use of AI and ADM systems involving personal data must comply with core data protection principles. These include ensuring that data is collected for specific and legitimate purposes, processed lawfully and appropriately, maintained with accuracy and security, and not retained longer than necessary.

Importantly, in 2023, Egypt introduced the Egyptian Charter for Responsible AI. This non-binding charter emphasises principles such as transparency, fairness and accountability in AI development and deployment. While it does not have legal force, it reflects Egypt’s commitment to fostering ethical AI practices and may influence future regulatory developments.

19.2 What guidance (if any) has/have the data protection authority(ies) issued in relation to the processing of personal data in connection with artificial intelligence?

While the PDPC has not yet issued specific regulatory guidance on AI, Egypt’s Second National AI Strategy 2025–2030 provides a forward-looking policy framework under Section 6.3 – Data Pillar, which addresses the intersection of AI and personal data protection.

Key provisions include:

- Comprehensive Data Governance (D-I6): The strategy calls for the development of robust data governance frameworks and standards for the collection, storage and use of data in AI systems. These frameworks are to include clear guidelines on data protection, privacy and consent, as well as mechanisms for data sharing and collaboration aligned with legal and ethical principles.
- Data Privacy and Security (D-I9): It outlines the establishment of a dedicated Personal Data Protection Authority (i.e. the PDPC) to monitor compliance, investigate data breaches and impose penalties. This includes enforcing industry-specific data standards, ensuring data interoperability and quality, and implementing enhanced security measures such as encryption, access controls, anonymisation and regular audits.
- Optimisation of the PDPL: The strategy explicitly calls for aligning Egypt’s PDPL with global best practices to ensure effective data privacy in AI applications. This includes introducing or refining regulations on data collection, storage, sharing, transparency and ethical AI use.⁴⁹

20 Trends and Developments

20.1 In your opinion, what enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.

Over the past 12 months, enforcement of Egypt’s PDPL has remained limited, primarily due to the delayed operation of the PDPC and the absence of finalised executive regulations. Consequently, there have been no formal administrative enforcement actions or penalties issued under the PDPL during this period.

Nonetheless, Egyptian courts have begun to address privacy-related disputes, particularly concerning the unauthorised dissemination of personal information via digital platforms.

Case example: dissemination of private information

In Case No. 19754 of 93 Judicial Year, dated 10 September 2024, the appellant was convicted of violating a victim’s privacy by disseminating private information and intentionally disturbing her by using communication devices. She challenged the judgment, citing insufficient reasoning, misinterpretation of evidence and a violation of her right to defence. The appellant argued that the judgment lacked clarity and failed to outline the crimes and evidence adequately, and should have been dismissed due to the plaintiff’s lack of standing. She also contended that her actions constituted permissible criticism and claimed the court ignored findings from an administrative investigation.

The Court of Cassation rejected the appellant’s claims, affirming that the judgment was legally sound, detailed and adequately reasoned. It upheld the conviction, dismissed objections to the admissibility of the case and ruled that the evidence supported the findings. The court also dismissed the appeal and ordered the forfeiture of the appellant’s bail, emphasising the importance of privacy rights and the clarity of judicial reasoning in such cases.

Significance of the case

This case illustrates important aspects of Egypt’s emerging privacy litigation landscape, including:

- the recognition of privacy violations – the court’s handling of this case highlights the growing seriousness with which privacy breaches involving personal information dissemination are being addressed; and
- judicial clarity and accountability – the Court of Cassation reinforced the need for clear, detailed reasoning in judgments related to privacy violations, ensuring accountability for misuse of personal data.

That said, we believe that privacy litigation in Egypt is gradually evolving, with courts increasingly addressing violations of personal data. Recent cases exemplify the judiciary’s commitment to protecting privacy rights, ensuring accountability for privacy violations, and upholding procedural fairness in such cases.⁵⁰

20.2 In your opinion, what “hot topics” are currently a focus for the data protection regulator?

As Egypt’s PDPC moves toward becoming operational, alongside the anticipated issuance of the executive regulations, we expect several regulatory priorities will shape its initial enforcement agenda:

- **AI and ADM:** The executive regulations and the PDPC are likely to address AI-driven profiling and ADM by promoting transparency, fairness and safeguards for Data Subjects.
- **Cross-Border Transfers:** With strict PDPL conditions on international data flows, the executive regulations are expected to oversee adequacy assessments, transfer approvals and possible localisation for sensitive personal data.
- **Consent and Transparency:** Greater scrutiny is anticipated around how consent is obtained and withdrawn, particularly in online advertising, biometric processing and children's data.
- **Digital Marketing and Tracking:** Regulatory attention is expected on profiling, cookie use and behavioural targeting practices to ensure lawful processing and opt-out options.
- **Children's Data and EdTech:** EdTech platforms will likely face requirements for parental consent, age verification and limits on commercial use of minors' data.
- **Enforcement Visibility:** The PDPC is expected to publish annual reports and support sector-specific codes of conduct to encourage accountability and transparency.
- **Security and Cooperation:** In line with Article 25, the PDPC is expected to coordinate with national and international authorities on cybersecurity incidents and cross-border investigations.

While formal enforcement is pending, these areas reflect Egypt's broader intent to align data protection with global best practices and ethical AI governance. Businesses should prepare now for PDPC-led oversight.

Endnotes

- 1 Articles 2, 3, 5, 6 and 7 of the PDPL. See also, <https://practiceguides.chambers.com/practice-guides/data-protection-privacy-2025/egypt>
- 2 Article 25 of the Telecommunications Law.
- 3 Article 2 of the Cybercrimes Law and Article 2 of its Executive Regulations.
- 4 Article 21 of the E-Signatures Law.
- 5 Article 12 of the E-Signatures Law Executive Regulations.
- 6 Articles 309bis and 309bis A of the Penal Code.
- 7 Article 25 of the Telecommunications Law.
- 8 Article 58 of the Telecommunications Law.
- 9 <https://practiceguides.chambers.com/practice-guides/data-protection-privacy-2025/egypt>
- 10 Article 1 of the PDPL.
- 11 <https://practiceguides.chambers.com/practice-guides/data-protection-privacy-2025/egypt>
- 12 Article 2-1 of the PDPL.
- 13 Article 3-1 of the PDPL.
- 14 Article 5-2 of the PDPL.
- 15 Article 6 of the PDPL.
- 16 Articles 4 and 5 of the PDPL.
- 17 Articles 3, 4.7 and 5.4 of the PDPL.
- 18 Articles 4. 2 and 4.8 of the PDPL.
- 19 Article 2 of the PDPL.
- 20 Article 9.6 of the PDPL.
- 21 Article 3 of the PDPL.
- 22 Article 4.7 of the PDPL.
- 23 Article 5.4 of the PDPL.
- 24 Articles 2, 4 and 5 of the PDPL.
- 25 Article 17 of the PDPL.
- 26 Article 33 of the PDPL.
- 27 The 14th chapter of the PDPL.
- 28 <https://practiceguides.chambers.com/practice-guides/data-protection-privacy-2025/egypt>
- 29 Articles 1 and 12 of the PDPL.
- 30 Articles 4.10, 5.11, 12, 14 and 16 of the PDPL.
- 31 Article 26 of the PDPL.
- 32 Article 27 of the PDPL.
- 33 Article 39 of the PDPL.
- 34 Article 5.1 of the PDPL.
- 35 <https://practiceguides.chambers.com/practice-guides/data-protection-privacy-2025/egypt>
- 36 Article 1 of the PDPL.
- 37 <https://practiceguides.chambers.com/practice-guides/data-protection-privacy-2025/egypt>
- 38 Article 14 of the PDPL.
- 39 <https://practiceguides.chambers.com/practice-guides/data-protection-privacy-2025/egypt>
- 40 Article 5 of the PDPL.
- 41 Articles 4 and 5 of the PDPL.
- 42 Articles 8 and 9 of the PDPL.
- 43 Article 33 of the PDPL.
- 44 Article 30 of the PDPL.
- 45 Articles 28 and 29 of the PDPL.
- 46 Article 34 of the PDPL.
- 47 Article 30 of the PDPL.
- 48 Articles 19 and 26 of the PDPL.
- 49 Egypt's National Artificial Intelligence Strategy Second Edition (2025–2030): https://mcit.gov.eg/Upcont/Documents/Publications_2212025000_National_AI_Strategy_Second_Edition_2025_2030.pdf
- 50 *Chambers Data Protection Privacy Guide 2025.*



Ibrahim Shehata has a decade of experience in the Egyptian market. He started off his career focusing on corporate law, where he successfully advised several multinational companies on doing business in Egypt, and has been involved in the Egyptian renewable energy market since 2014, developing niche expertise that makes him one of the leading lawyers in the field. He is also recognised as one of the key players in the entrepreneurial ecosystem, having worked with more than 60 start-ups. In this regard, Shehata has helped start-ups navigate the legal issues that always arise in this specific realm and guided them to be more investment ready.

Shehata & Partners

Cairo Business Plaza, North Tower, 2nd Floor, Unit (204)
New Cairo, Cairo
Egypt

Tel: +20 102 225 6100
Email: is@shehatalaw.com
LinkedIn: www.linkedin.com/in/ibrahim-shehata-8698258b



Tasneem ElNaggar is a Mid-Level Associate at Shehata & Partners with expertise in corporate law, commercial transactions and regulatory compliance. She interned at several top-tier Egyptian law firms before beginning her career in arbitration at Khodeir & Partners. She holds a diploma in Public Law from Ain Shams University and is currently pursuing her Master's degree. Tasneem has advised on major projects, including Yazaki's private free-zone establishment in Egypt, and has supported emerging fintech ventures. Her experience spans diverse fields, from drafting contracts for a theatrical production in Saudi Arabia to advising AI-driven startups, demonstrating her adaptability across industries.

Shehata & Partners

Cairo Business Plaza, North Tower, 2nd Floor, Unit (204)
New Cairo, Cairo
Egypt

Tel: +20 102 011 8038
Email: tn@shehatalaw.com
LinkedIn: www.linkedin.com/in/tasneem-elnaggar-135946220



Safa Rabea recently joined Shehata & Partners, specialising in corporate governance and commercial law. She previously completed internships at top-tier law firms, gaining valuable experience in banking and finance, arbitration and M&A transactions. She then joined Al-Hussien and Partners, where she advised on corporate transactions, compliance and risk management, further strengthening her legal expertise.

Shehata & Partners

Cairo Business Plaza, North Tower, 2nd Floor, Unit (204)
New Cairo, Cairo
Egypt

Tel: +20 114 045 4669
Email: sr@shehatalaw.com
LinkedIn: www.linkedin.com/in/safa-rabea

Shehata & Partners was founded in 1996 and has been driven by a vision to provide unique legal services that cater to the business needs of corporate entities doing business in Egypt. Its core mission is to provide the most trusted and effective legal advice on both dispute resolution and corporate law in Egypt. The firm is result-driven and delivers exceptional services to clients across various practice areas and multiple industries. It continues to achieve the highest client satisfaction rates in the region due to the meticulous implementation of its client-centric approach.

www.shehatalaw.com



France



Clara Hainsdorf



Bertrand Liard

White & Case LLP

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

Since 25 May 2018, the main data protection legislation in the EU has been Regulation (EU) 2016/679 (“General Data Protection Regulation” or “GDPR”).

Since 6 January 1978, the French Data Protection Act (“FDPA”) has been in force, as amended on 20 June 2018 and completed by two decrees of 1 August 2018 and 12 December 2018 to implement the requirements of the GDPR under French law.

1.2 Is there any other general legislation that impacts data protection?

Directive 2002/58/EC (as amended by Directive 2009/136/EC) (“ePrivacy Directive”), pending the ePrivacy Regulation, was implemented by the laws of 21 June 2004, 9 July 2004 and 6 August 2004. This directive was intended to be replaced by the ePrivacy Regulation, which was reportedly abandoned by the European Commission, as stated in a *communiqué* issued on 12 February 2025.

Additional legislation impacting data protection are:

- Directive 2016/680 on the processing of personal data by competent authorities, implemented under French law in 2018 (law of 20 June 2018 and Decree of 1 August 2018);
- Articles L.34-1 *et seq.* of the Post and Electronic Communication Code (“PECC”);
- Articles 226-16 *et seq.* of the French Criminal Code (“FCC”) on infringements of the rights of the individual resulting from computer files or processing;
- Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector;
- Regulation (EU) 2022/2065 on a Single Market for Digital Services;
- Regulation (EU) 2023/2854 of the European Parliament and of the Council on harmonised rules on fair access to and use of data;
- Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union (NIS 2), which has not been transposed to this date;
- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (“AI Act”); and

- Regulation (EU) 2024/2847 of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements.

1.3 Is there any sector-specific legislation that impacts data protection?

The GDPR and FDPA apply to all sectors, but the French data protection authority (“CNIL”) publishes numerous recommendations and guidelines focused on specific sectors (e.g., health, insurance, HR, whistleblowing, etc.).

1.4 What authority(ies) are responsible for data protection?

The CNIL, whose mission is to ensure that data privacy laws are properly applied and, to some extent, the French authority responsible for competition and consumer law (“DGCCRF”).

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

The key definitions are set out in Article 4 of the GDPR, as incorporated into French law by Article 3 of the FDPA:

- **“Personal Data”** means any information that identifies, directly or indirectly, a person – such as a name, ID number, location, online identifier or personal characteristics.
- **“Processing”** refers to any operation on personal data, automated or not, including collection, storage, use, disclosure, adaptation, restriction or deletion.
- **“Controller”** means the natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data.
- **“Processor”** means a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller.
- **“Data Subject”** means an individual who is the subject of the relevant personal data.
- **“Sensitive Personal Data”/“Special Categories of Personal Data”** are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning

health or sex life or sexual orientation, genetic data or biometric data.

- **“Data Breach”** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

3 Territorial and Material Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The GDPR applies to non-EU businesses if they are subject to Member State law under public international law, or if they process EU residents’ data in connection with offering goods/services or monitoring behaviour within the EU.

Under Article 3 of the FDPA, French law applies to processing linked to a controller’s or processor’s activities in France, regardless of establishment location. Article 3(II) further provides that national GDPR-implementing rules apply when the data subject resides in France, except for processing related to journalistic, academic, artistic or literary expression, where the law of the controller’s Member State applies.

3.2 Do the data protection laws in your jurisdiction carve out certain processing activities from their material scope?

The GDPR explicitly excludes certain activities from its scope under Article 2, §2, including the following:

- Processing carried out in activities not subject to EU law.
- Processing carried out by Member States within the framework of policies regarding border controls, asylum and immigration defined in Chapter II of Title V of the EU Treaty.
- Personal or domestic processing carried out by a natural person.
- Processing carried out by competent authorities for the prevention, detection and prosecution of criminal offences, as well as for the enforcement of criminal sanctions, including the protection of public security and the prevention of threats to such security.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
Personal data must be processed lawfully, fairly and in a transparent manner. Controllers must provide certain minimum information to data subjects regarding the collection and further processing of their personal data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
- **Lawful basis for processing**
Personal data may be processed only if permitted under EU law. Article 5 of the FDPA sets out the main legal bases, as follows: consent; contractual necessity; legal obligation; or legitimate interest. Sensitive data processing is allowed under strict conditions, such as explicit consent, employment law or legal claims.

- **Purpose limitation**

Personal data must be collected for specific, explicit and legitimate purposes, and not used incompatibly. If reused for new purposes, the controller must inform the data subject and ensure a valid legal basis applies.

- **Data minimisation**

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed.

- **Proportionality**

Data processing activities must be justified and balanced, ensuring that only necessary personal data is collected and processed in relation to the intended purpose.

- **Retention**

Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

- **Accuracy**

Personal data must be accurate and, where necessary, kept up to date. A business must take every reasonable step to ensure that personal data that are inaccurate are either erased or rectified without delay.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

The rights of individuals are set out in the GDPR and further incorporated into French law through Articles 104 to 110 of the FDPA:

- **Right of access to (copies of) data/information about processing**
A data subject has the right to obtain from a controller information in respect of the processing of his/her personal data. The data subject may request a copy of the personal data being processed.
- **Right to rectification of errors**
Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data subjects have the right to rectification of inaccurate personal data.
- **Right to deletion/right to be forgotten**
Data subjects have the right to erasure of their personal data (“right to be forgotten”).
- **Right to object to processing**
Data subjects may object to processing based on public or legitimate interest. The controller must stop unless it demonstrates overriding grounds or needs the data for legal claims.
- **Right to restrict processing**
Data subjects have the right to restrict the processing of personal data, which means that the data may only be held by the controller and may only be used for limited purposes.
- **Right to data portability**
Data subjects can receive their data in a machine-readable format and transfer it between controllers or request direct transmission.
- **Right to withdraw consent**
Data subjects may withdraw consent at any time without affecting prior processing. They must be informed of this right, and withdrawal must be as easy as giving consent.

- **Right to object to marketing**
Data subjects have the right to object to the processing of personal data for the purpose of direct marketing, including profiling.
- **Right protecting against solely automated decision-making and profiling**
Data subjects may not be subject to solely automated decisions with legal effects, except where necessary for a contract, based on explicit consent, or compliant with Article L.311-3-1 of the Public Administration Code.
- **Right to complain to the relevant data protection authority(ies)**
Data subjects have the right to lodge complaints concerning the processing of their personal data with the CNIL, if the data subjects live in France or the alleged infringement occurred in France.
- **Right to information**
Data subjects have the right to be provided with information on the identity of the controller, the reasons for processing their personal data and other relevant information necessary to ensure the fair and transparent processing of personal data.
- **Right to set guidelines for the retention, deletion and disclosure of personal data after a data subject's death**
Individuals may set general or specific guidelines on the handling of their personal data after death. In principle, such data may be processed unless the person objected during their lifetime.

5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

A class action may be brought either to prevent continuation of the breach, or to obtain compensation for the harm suffered (or both). A class can only be represented by:

- an association that has existed for at least five years, whose statutory purpose includes the defence of the infringed interests;
- an approved consumer association; or
- certain trade union organisations.

The CNIL must be informed by the applicant on behalf of the class.

6 Children's Personal Data

6.1 What additional obligations apply to the processing of children's personal data?

To lawfully process the personal data of a minor under 15 years old, consent must be given jointly by the minor concerned and the person(s) having parental authority over such minor (Article 45 FDPA). However, the CNIL Recommendation No. 4 (which is not imperative) indicates that it is sufficient for the online service provider to obtain the consent of only one of the two parents.

French law does not provide for specific methods to validly obtain consent of a parent or legal guardian. The controller must make reasonable efforts to verify that consent has been given by the holder of parental responsibility.

In addition, the "SREN" Law (Law No. 2024-449 of 21 May 2024) imposes specific obligations on online services legally restricted to users aged 18 or over, such as pornographic websites or platforms with content deemed manifestly inappropriate for minors. This system must ensure effective age control while preserving user anonymity and preventing the

storage or access to any identity or age-related data by the service provider.

7 Registration Formalities and Prior Approval

7.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

There is no longer an obligation on businesses to register with or notify the CNIL since the GDPR came into force. However, this obligation has been replaced by the obligation to keep a record by the controller or, where applicable, its representative.

Only a limited number of formalities remain, notably in the health sector and for specific cases requiring prior opinion.

7.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

If such registration or notification is needed, the level of detail depends on the applicable procedure. Where the processing falls under a pre-approved framework (such as a CNIL reference framework or methodology), only a simplified declaration may be required. Otherwise, a full prior authorisation request must be submitted, providing detailed information on the data processed, purposes, legal basis, security measures, data retention, and – where applicable – risk assessments and ethics approvals.

7.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

Registrations or notifications are made per processing operation in cases requiring prior authorisation. However, where the processing is covered by a CNIL reference framework or methodology, a single declaration of conformity may cover all relevant processing operations carried out by the data controller that fall under the scope of that framework.

7.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

If the controller is established in France, it must notify the CNIL directly. If the controller is not established in the EU but falls within the territorial scope of the GDPR (Article 3(2)), it must designate a representative in the EU, who may handle such formalities on its behalf.

7.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

When prior notification is required, the controller must

provide key information about the processing, including its identity, purposes, categories of data and data subjects, retention periods, security measures, and, if applicable, transfers outside the EU. If the controller is not established in the EU, the notification must also include the identity and contact details of its designated representative in France.

7.6 What are the sanctions for failure to register/notify where required?

Failure to obtain prior authorisation for a data processing operation subject to such a requirement may result in up to one year of imprisonment and a fine of €300,000, pursuant to Article 226-16 of the French Penal Code. In addition, unlawful processing under the GDPR may give rise to administrative fines of up to €20 million or 4% of the global annual turnover, pursuant to Article 83(5) of the GDPR.

7.7 What is the fee per registration/notification (if applicable)?

There is no fee. Registration and notification are free of charge.

7.8 How frequently must registrations/notifications be renewed (if applicable)?

Registrations or notifications to the CNIL are generally not subject to periodic renewal. A new authorisation is only required if the processing undergoes a substantial change, such as a modification of its purpose, the categories of data processed or the technical means used.

7.9 Is any prior approval required from the data protection regulator?

Yes, prior approval from the CNIL is still required in limited cases, despite the general shift to accountability under the GDPR. This concerns certain sensitive processing operations, such as the use of genetic data for research purposes, biometric data for access control to secure areas, or the processing of the national identification number (NIR) outside legally defined exceptions.

7.10 Can the registration/notification be completed online?

Yes, registration and notification procedures can be completed online via the CNIL's dedicated teleservice. This includes standard notifications, requests for prior authorisation and other formalities required under French data protection law.

7.11 Is there a publicly available list of completed registrations/notifications?

Yes, a publicly available list of completed registrations and notifications is accessible online. Datasets are published on <https://www.data.gouv.fr>, and include all data processing operations subject to prior formalities since 25 May 2018.

7.12 How long does a typical registration/notification process take?

For prior authorisations, the CNIL must respond within two months, extendable once to four months. If no decision is issued within that time, the request is generally considered tacitly approved.

8 Appointment of a Data Protection Officer

8.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The appointment of a DPO is only mandatory as set out in Article 37(1) of the GDPR, including where there is: (i) large-scale regular and systematic monitoring of individuals; or (ii) large-scale processing of sensitive personal data.

Where a business designates a DPO voluntarily, the requirements of the GDPR apply as though the appointment were mandatory.

8.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

Where appointment of a DPO is mandatory, failure to comply may result in a wide range of penalties available under the GDPR.

8.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

The appointed DPO should not be dismissed or penalised for performing their tasks and should report directly to the highest management level of the controller or processor.

8.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

A single DPO is permitted by a group of undertakings provided that the DPO is easily accessible from each establishment.

8.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The DPO should be appointed on the basis of professional qualities and should have an expert knowledge of data protection law and practices. While this is not strictly defined, it is clear that the level of expertise required will depend on the circumstances.

8.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

A DPO should be involved in all issues involving personal data, e.g.: (i) monitoring compliance with the GDPR with internal

policies including internal audits; (ii) advising on Data Protection Impact Assessments (“DPIAs”) and the training of staff; and (iii) co-operating with the CNIL and acting as the authority’s primary contact.

8.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

Yes, the appointment of a DPO must be registered/notified with the relevant data protection authority.

8.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

The DPO does not necessarily need to be named in the public-facing privacy notice, but the WP29 (now the European Data Protection Board “EDPB”) recommends that both the CNIL and employees should be notified of the DPO’s name and contact details.

9 Appointment of Processors

9.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes, the business must enter into a form of agreement with a processor.

9.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

Article 122 of the FDPA, in accordance with Article 28 of the GDPR, states that the processor must be appointed under a binding agreement in writing. The contractual terms must notably stipulate that the processor: (i) only acts on the documented instructions of the controller; (ii) imposes confidentiality obligations on all employees; and (iii) ensures the security of personal data that it processes.

10 Marketing

10.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

For email or SMS marketing to consumers, consumers must give their prior opt-in consent and be informed, at the time of the collection of the email address or phone number, that such personal data will be used for marketing purposes (Article L34-5 PECC). However, opt-out consent applies if: (i) the recipient is already a customer of the advertiser and if the marketing message concerns similar products or services provided by the same company; or (ii) the prospecting is not of a commercial nature.

Additionally, Article L121-34 of the French Consumer Code prohibits unsolicited direct marketing calls to individuals registered on the national opt-out list (Bloctel), subject to certain exceptions.

10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

These restrictions are only applicable to business-to-consumer marketing. For business-to-business marketing, opt-out consent applies. Indeed, the principle is that direct marketing can be based on the legitimate interest of the organisation. However, the individual must, at the time of collection of his/her e-mail address: (i) be informed that his/her e-mail address will be used for the purpose of electronic prospecting; and (ii) be able to object to such use in a simple and free manner.

10.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

Direct marketing by post or telephone is possible on the condition that individuals are, at the time of collection of their postal address and/or telephone number: (i) informed of the use of their data for prospecting purposes; and (ii) able to object to this use in a simple and free manner.

Advertising via automatic calling machines is possible provided that data subjects have explicitly given their consent before being contacted.

Additionally, a law adopted in May 2025 mandates prior explicit consent for any commercial telephone calls to consumers, effective from 11 August 2026.

10.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Yes, they apply to all marketing sent to users located in France.

10.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

Yes. On 12 October 2023, the CNIL fined GROUPE CANAL+ €600,000 for electronic marketing without valid consent. Consent forms from its partners lacked clear information on data recipients.

On 4 April 2024, HUBSIDE.STORE was fined €525,000 for using data from brokers without valid consent. Specialised in telemarketing, the company’s use of such data was deemed illegal.

On 15 May 2025, the CNIL fined Solocal Marketing Services €900,000 for processing prospect data obtained via data brokers without ensuring valid opt-in consent under Article L.34-5 of the PECC, and ordered it to cease operations under threat of a €10,000 daily fine.

Additionally, breaches of Article 34-5 of the PECC concerning marketing are sanctioned by the DGCCRF.

10.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Yes, provided that:

- (i) the file sold contains only the data of active customers who have not objected to the transmission of their data

- in the case of postal or telephone canvassing or who have consented to it in the case of electronic canvassing; and
- (ii) the purchaser informs the data subjects concerned and is able to demonstrate that he/she has their informed consent for electronic marketing.

Additionally, following a CNIL publication on 23 January 2025 regarding the reuse of databases, the purchaser must perform statutory verifications – including confirming the legality and licit origin of each dataset, as well as ensuring that the original consent covers the intended marketing purposes – before relying on consent under Article L.34-5 of the French Postal and Electronic Communications Code.

10.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Breaches of data are punishable by an administrative penalty issued by the DGCCRF, which may not exceed €75,000 for a natural person and €375,000 for a legal entity (Article L.34-5 PECC). The CNIL may also impose GDPR-based sanctions “up to the higher of 4% of the total worldwide annual turnover or €20 million”.

The FCC also provides for a criminal penalty of up to five years of imprisonment and a maximum fine of €300,000 for natural persons or €1.5 million for legal entities, for processing personal data for direct marketing purposes despite the objection of the data subject (Article 226-18-1 FCC).

11 Cookies

11.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

Under Article 82 of the FDPA (implementing Article 5 of the ePrivacy Directive), storing cookies on a user’s device requires prior consent that is informed, specific, freely given and unambiguous. This excludes technical cookies.

The CNIL regularly updates its cookie guidance, most recently on 4 November 2022.

On 17 January 2023, the CNIL and other EU DPAs adopted a joint report on cookie banners, following complaints by NOYB. Although cookies fall under the ePrivacy Directive, the EDPB deemed coordinated action necessary due to the volume and cross-border nature of the complaints.

11.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

The requirement to inform the user and to obtain the user’s consent applies to all cookies, except those which: (i) have the sole purpose of enabling or facilitating communication by electronic means; or (ii) are strictly necessary for the provision of an online communication service at the express request of the user.

With regard to cookies that are not subject to consent, we can notably mention:

- logs that preserve the choice expressed by users on the deposit of tracers;
- logs intended for authentication to a service; and
- logs for personalising the user interface.

11.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

On 29 December 2023, the CNIL fined YAHOO EMEA LIMITED €10 million for failing to respect the choices of internet users who refused cookies on its “Yahoo.com” website and for not allowing users of its “Yahoo! Mail” service to freely withdraw their consent to cookies.

On 14 November 2024, the French telecommunications company Orange was sanctioned by the CNIL with a fine of €50 million, notably for having implemented cookies on its website without obtaining users’ consent.

Shortly thereafter, on 12 December 2024, the CNIL issued formal notices to several website operators, requiring them to modify their cookie banners, which were deemed misleading.

11.4 What are the maximum penalties for breaches of applicable cookie restrictions?

The maximum penalty is the higher of €20 million or 4% of worldwide turnover. Moreover, the FCC provides a penalty of five years of imprisonment and a fine of €300,000 or €1.5 million for legal entities in the case of collection of data by fraudulent, unfair or unlawful means (Article 226-18 FCC).

12 Restrictions on International Data Transfers

12.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Data transfers are not subject to restrictions beyond those set out in the GDPR.

12.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

Businesses typically rely on the Standard Contractual Clauses (“SCCs”) drafted by the EU Commission or the implementation of Binding Corporate Rules (“BCRs”). BCRs will always need approval from the CNIL and must include a mechanism to ensure they are legally binding and enforced by every member in the group. The other mechanisms set out in the GDPR are more rarely used.

Since 10 July 2023, the Data Protection Framework (“DPF”) has governed EU–US data transfers. It includes an annual certification regime and a right of appeal via the new Data Protection Review Court. In its 2024 review, the EDPB raised concerns over the DPF’s effectiveness, urging ongoing monitoring and conditional adequacy based on the safeguards’ implementation.

12.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

BCRs must be approved by the CNIL where the leading entity

is subject to the FDPA, which can take several years. Transfers based on legitimate interest also require prior approval from the CNIL.

12.4 Do transfers of personal data to other jurisdictions require a transfer impact assessment? If conducting a transfer impact assessment is only mandatory in some circumstances, please identify those circumstances.

Following the “Schrems II” decision, the CNIL provided guidance and recommended to: (i) record all data transfers of the organisation, divided into a technical and contractual part; and (ii) define an action plan that includes a risk assessment.

The EDPB issued recommendations on 18 June 2021 on measures that complement transfer instruments to ensure compliance with the EU level of protection of personal data. These recommendations provide data exporters with a methodology to follow in order to assess the level of protection of third countries and to determine whether and which additional measures should be put in place.

12.5 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in Schrems II (Case C-311/18)?

The CNIL provides guidance on how to implement the new SCCs published by the European Commission on 4 June 2021 (“2021 SCCs”) into contracts concluded after 27 September 2021: identification of the types of data transfers and the relevant SCCs; completion of the SCCs and its appendix; and completion of the necessary steps with the CNIL. In January 2025, the CNIL also published the final version of its Data Transfer Impact Analysis guide, providing a structured method to assess third-country laws and define supplementary measures to ensure adequate data protection.

12.6 What guidance (if any) has/have the data protection authority(ies) issued in relation to the use of standard contractual/model clauses as a mechanism for international data transfers?

The “2021 SCCs” replace the SCCs adopted under the Data Protection Directive (“2010 SCCs”). Until 27 December 2022, controllers and processors could continue to rely on the 2010 SCCs for contracts that were concluded before 27 September 2021. For contracts concluded after 27 September 2021, the 2021 SCCs must be incorporated.

13 Whistle-blower Hotlines

13.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

Under French Law No. 2022-401 of 21 March 2022, whistle-blowing may concern crimes, misdemeanours, threats to the public interest, or violations of international, EU or national law. However, disclosures breaching national defence secrecy,

medical confidentiality or legal professional privilege are excluded from the alert system.

On 18 July 2019, the CNIL adopted a reference framework on professional alert systems, updated in July 2023 to reflect GDPR implementation. Key updates include: (i) coverage of alerts stemming from legal obligations (e.g. “duty of care”, “Sapin II”) and those initiated by controllers (e.g. ethical alerts); (ii) a unified framework for all alert systems to enhance clarity for data subjects; and (iii) clarification of data retention rules. A further update is expected following recent changes to the “Sapin II” law.

13.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous reporting is not prohibited; however, the CNIL strongly discouraged it by conditioning it to the following conditions:

- (i) the seriousness of the facts mentioned must be established and the factual elements must be sufficiently detailed; and
- (ii) the processing must be surrounded by specific precautions, such as a preliminary examination, by the first addressee of the appropriateness of its dissemination within the framework of the system.

14 CCTV

14.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

A DPIA is required, with DPO input, for large-scale systematic monitoring of publicly accessible areas. If the DPIA indicates a high risk to individuals’ rights, the controller must consult the data protection authority before proceeding.

The controller must submit details of responsibilities, processing purposes, the DPIA, applicable safeguards under the GDPR, and DPO contact information.

If the authority considers the processing non-compliant, it must issue written advice within eight weeks and may exercise its broader investigative and corrective powers under the GDPR.

14.2 Are there limits on the purposes for which CCTV data may be used?

The CNIL has published several guidelines on CCTV prohibiting filming employees at their workstations or during their break or in rest areas, or toilets, and filming public highways (as opposed to the immediate surroundings of their buildings in places likely to be exposed to acts of terrorism).

The CNIL specifies that before installing video surveillance cameras in public places, obtaining prior authorisation from the prefecture is mandatory (Code of Internal Security, Article R252-11).

15 Employee Monitoring

15.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Employee working time may be monitored if the tools used are proportionate and respect privacy. Employers may:

- Use screen and phone recordings in limited professional contexts (e.g. training), with strict access controls.
- Record calls for training, evaluation, quality improvement or contractual evidence.
- Use geolocation in professional vehicles when justified (e.g. billing, safety or tracking work hours when no alternative exists).

Each measure must be necessary for the stated purpose and implemented with appropriate safeguards.

15.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Consent of employees is rarely used as a valid ground to process personal data due to the subordination link with the employer.

Employees must be informed in advance of any monitoring of their work, which usually means through an internal note as the employer is supposed to keep a proof of this information to validly bind the employee upon internal rules and regulations.

More generally, all data subjects (employees and visitors) must be adequately informed, by means of signs posted permanently in a visible way in the locations concerned, which include at least, in addition to the pictogram of a camera, indicating that the location is placed under video protection.

15.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

The employer must comply with its obligation of transparency and loyalty towards its employees.

Consequently, after having informed and consulted the employee representatives about the monitoring systems, it must inform the employees directly by any means that will allow him/her to ensure that they are aware of the information transmitted (e.g., an internal note with acknowledgment of receipt).

15.4 Are employers entitled to process information on an employee's attendance in office (e.g., to monitor compliance with any internal return-to-office policies)?

Under French labour law, employers may monitor employees but cannot impose constant surveillance unless strictly necessary due to the nature of the task. For example, requiring an employee to remain permanently on webcam to verify their presence is considered excessive, as less intrusive means exist for ensuring security or monitoring hours. Similarly, continuous screen sharing or the use of keyloggers constitutes disproportionate surveillance.

On 27 December 2023, the CNIL fined AMAZON FRANCE LOGISTIQUE €32 million for using an excessively intrusive monitoring system without proper employee information or security measures. In December 2024, the CNIL issued formal notices for unlawful real-time video surveillance in public spaces, reaffirming the principle of proportionality.

16 Data Security and Data Breach

16.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

According to Article 121 of the FDPA, personal data must be processed securely to prevent unauthorised or unlawful access, loss, destruction or damage. Controllers and processors must adopt appropriate technical and organisational measures under the GDPR. These may include encryption, ensuring ongoing system confidentiality and resilience, restoring access after incidents and regularly testing security systems.

Regarding employee data, the CNIL recommends that employers only request information necessary for work tasks, restrict access to sensitive data such as bank details while logging any actions taken, and always inform employees when requesting personal data. These principles help ensure lawful and proportionate handling of employee information.

16.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

The controller must report any personal data breach to the data protection authority without undue delay, and no later than 72 hours after becoming aware of it, unless the breach is unlikely to pose a risk to data subjects' rights. Processors must notify the controller without delay. The notification must detail the breach's nature, affected data subjects, contact details of the DPO, likely consequences and mitigation measures.

In case of security incidents, operators of vital or essential services, digital platforms and telecom providers must also notify the French Cybersecurity Agency (ANSSI).

If health data is involved, the Regional Health Agency (ARS) must be informed as well.

16.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Controllers have a legal requirement to communicate the breach to the data subject, without undue delay, if the breach is likely to result in a high risk to the rights and freedoms of the data subject.

The notification must include the name and contact details of the DPO (or point of contact), the likely consequences of the breach and any measures taken to remedy or mitigate the breach.

The controller may be exempt from notifying the data subject if the risk of harm is remote (e.g., because the affected data is encrypted), the controller has taken measures to minimise the risk of harm (e.g., suspending affected accounts) or the notification requires a disproportionate effort (e.g., a public notice of the breach).

16.4 What are the maximum penalties for personal data security breaches?

Under the GDPR, the maximum penalty is the higher of €20 million or 4% of worldwide turnover.

Moreover, Article 226-17-1 of the French Penal Code provides that the failure of an electronic communications service provider or data controller to notify a personal data breach is punishable by five years' imprisonment and a fine of €300,000.

17 Enforcement and Sanctions

17.1 Describe the enforcement powers of the data protection authority(ies).

- (a) **Investigative powers:** The authority may request any information, conduct audits, review GDPR certifications, notify infringements, and access personal data and premises, including processing equipment. These powers apply to both controllers and processors. No criminal sanctions are foreseen.
- (b) **Corrective powers:** The data protection authority may issue warnings, order disclosure of data breaches, ban processing, withdraw certifications and impose administrative fines. These powers aim to ensure compliance. No criminal sanctions are provided for under current data protection law.
- (c) **Authorisation and advisory powers:** The data protection authority may advise controllers, accredit certification bodies and authorise certificates, clauses, arrangements and BCRs under the GDPR. No criminal sanctions apply.
- (d) **Imposition of administrative fines for infringements of specified legal provisions:** The GDPR provides for administrative fines, which can be €20 million or up to 4% of the business's worldwide annual turnover of the preceding financial year. No criminal sanctions apply.
- (e) **Non-compliance with a data protection authority:** The GDPR provides for administrative fines, which can be €20 million or up to 4% of the business's worldwide annual turnover of the preceding financial year, whichever is higher. No criminal sanctions apply.

17.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The GDPR entitles the relevant data protection authority to impose a temporary or definitive limitation including a ban on processing.

17.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

The CNIL conducts investigations mainly following complaints or data breach notifications. In other cases, it initiates control operations to identify failures before deciding on appropriate sanctions.

The CNIL intervenes in different ways: it can either give formal notice to comply to the entity concerned; or decide to sanction it immediately.

In addition, each year the CNIL defines a thematic control programme. In line with its new 2025–2028 strategic plan, the CNIL announced that future enforcement priorities will include the supervision of emerging uses of AI, digital health, smart surveillance technologies and the processing of children's data. Additionally, in early 2025, the CNIL stated that it would strengthen its enforcement actions following the numerous data breaches reported in 2024.

17.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

The CNIL exercises its powers against any international entity as soon as the breaches at issue concern personal data of French data subjects. In this context, the CNIL has already had the opportunity on several occasions to impose a penalty on an entity whose head office is not located in France when French users were concerned.

On 20 October 2022, the CNIL imposed a fine of €20 million on the US company CLEARVIEW AI. The company was ordered to cease collecting and using data from individuals in France without legal basis.

18 E-discovery/Disclosure to Foreign Law Enforcement Agencies

18.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Companies must follow cross-border transfer rules but also the CNIL's recommendation of 23 July 2009, explaining how to answer the questions of companies involved in lawsuits in the United States.

In addition, the French blocking statute (1968) prevents the transmission of information to foreign courts outside the channels set forth by treaties (such as the 1970 Hague Convention for civil matters or the mutual legal assistance treaties for criminal issues). Although rarely applied so far, the statute was recently amended in 2022 to have companies receiving requests that may fall within the scope of the blocking statute inform the Strategic Information and Economic Security Service.

18.2 What guidance has/have the data protection authority(ies) issued on disclosure of personal data to foreign law enforcement or governmental bodies?

The CNIL made several recommendations including, in 2009, to recall that the required transfers of information must necessarily be carried out in accordance with the Hague Convention, the only international convention linking France to the United States in terms of legal proceedings.

19 Artificial Intelligence

19.1 Are there any limitations on automated decision-making involving the processing of personal data using artificial intelligence?

Article 22(1) of the GDPR gives individuals the right not to be subject to solely automated decision-making, including

profiling, that produces legal or similarly significant effects. Such decisions, including those made by AI without human involvement, are generally prohibited.

Under Article 22(2), exceptions apply where the processing is necessary for a contract or based on the individual's explicit consent. Even in these cases, businesses must implement safeguards to protect the individual's rights and interests, including the right to obtain human intervention, express their views and challenge the decision.

In parallel, the AI Act introduces further obligations for high-risk AI systems, including those involving automated decision-making – except where the system does not substantially affect the outcome, as clarified in Recital 53. Under Article 6 and Annex III, such systems – used in contexts like employment, education or access to public services – must comply with strict requirements, including risk management (Article 9), technical documentation (Article 11), and human oversight (Article 14). Transparency is also required under Article 52, ensuring that individuals are informed when an AI system significantly influences decisions concerning them.

19.2 What guidance (if any) has/have the data protection authority(ies) issued in relation to the processing of personal data in connection with artificial intelligence?

The EDPB published guidelines on 10 April 2025 addressing personal data use in AI and blockchain, reaffirming core GDPR principles and calling for clear role definitions, DPIAs and safeguards such as explainability, access controls and audits.

On 18 December 2024, the EDPB also issued an opinion on AI model training and deployment, outlining lawful bases for each stage and stressing the need for compatibility, transparency and safeguards, particularly for public data.

At the national level, the CNIL has issued several practical resources to support GDPR-compliant AI development. On 18 July 2024, it published guidance and a FAQ on generative AI, urging organisations to clearly define use cases, avoid sensitive data, and favour secure or on-premises hosting. On 7 February 2025, it issued recommendations on transparency, notably addressing the need to inform individuals when their data is used to train AI models. Most recently, on 11 April 2025, it published the results of its AI sandbox on public sector use cases.

20 Trends and Developments

20.1 In your opinion, what enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.

In 2024, data protection enforcement across Europe remained strong, with GDPR fines reaching €1.2 billion. Authorities

increasingly favoured coordinated actions. The EDPB's investigation into access rights exposed systemic shortcomings, while the CNIL's 2025–2028 strategy emphasises greater involvement in cross-border cases, particularly those concerning digital platforms and AI.

Children's data remains a priority. The Data Protection Commission's €345 million TikTok fine in 2023 resonated EU-wide and mirrored the CNIL's concern over youth data protection.

Another key trend is the growing focus on cybersecurity and data breaches. In early 2025, the CNIL announced reinforced enforcement following a 20% rise in breach notifications in 2024, including several large-scale incidents. The annual report confirmed a record number of corrective actions and €55 million in fines, some specifically for security failures.

Additionally, in 2024, CNIL inspections revealed persistent misuse of trackers – including unclear banners and premature data collection. Formal notices and fines followed, notably against major adtech firms, for failing to ensure refusal of consent is as simple as acceptance. EU regulators share a common stance: tracking must be lawful and genuinely consensual.

The CNIL also investigates generative AI for GDPR compliance on transparency and purpose limitation, reflecting broader EU concerns. It also monitors biometric surveillance at work, targeting facial recognition and emotion-detection tools.

20.2 In your opinion, what "hot topics" are currently a focus for the data protection regulator?

Regulatory priorities in France and across Europe show a blend of principle and pragmatism.

Online child protection has become a top priority. In February 2025, the EDPB set 10 principles for age assurance, stressing proportionality, effectiveness and privacy. The CNIL adopted them in its 2024 roadmap, launching inspections on youth-targeted platforms and advocating designs that protect without profiling. Cases like TikTok show that age-appropriate design is becoming essential.

Data security and breach prevention have also gained prominence. Following a sharp rise in large-scale breaches in 2024, the CNIL reinforced its enforcement strategy in early 2025, issuing guidance on securing large datasets and promoting multi-factor authentication and regular audits for high-risk processing.

Note

This publication is provided for your convenience and does not constitute legal advice. This publication is protected by copyright.



Clara Hainsdorf is a partner in the Intellectual Property and Information Technology department at White & Case's Paris office. She advises international and domestic clients across sectors such as social media, finance, hospitality, automotive, and food and beverages. Clara has in-depth expertise in information and communication technology law, including technology licensing, e-commerce, social media, and complex industrial and commercial contracts. She assists clients in both contentious and non-contentious matters, with a particular focus on privacy and data protection, especially in cross-border contexts. She has significant experience interacting with the French data protection authority (CNIL) and other European regulators. She is co-author of major White & Case publications, including the *GDPR Handbook* and the *GDPR National Implementation Guide*. Clara frequently speaks on privacy, technology and fintech issues and was a speaker at Viva Technology 2023. She joined White & Case in 2005, following experience at international law firms in New York and Paris.

White & Case LLP
19, Place Vendôme
75001 Paris
France

Tel: +33 1 55 04 58 52 / +33 1 55 04 15 15
Email: chainsdorf@whitecase.com
LinkedIn: www.linkedin.com/in/clara-hainsdorf-90515733



Bertrand Liard is a partner at White & Case's Paris office, where he leads the Intellectual Property and Information Technology department. He has broad expertise in intellectual property, IT, data protection and cybersecurity. Bertrand advises international clients from sectors such as social media, advertising, transport, luxury goods, industry and finance, with a focus on fintech. He assists with cross-border litigation, compliance and technology transactions. Renowned for his strategic input in complex data and technology disputes, Bertrand often crafts innovative legal arguments and contributes to setting new precedents. He regularly speaks and publishes on privacy, technology and fintech topics. Bertrand joined White & Case in 2007 from another major international law firm. *Chambers Europe* has ranked him for over a decade in TMT: Information Technology.

White & Case LLP
19, Place Vendôme
75001 Paris
France

Tel: +33 1 55 04 15 03
Email: bertrand.liard@whitecase.com
LinkedIn: www.linkedin.com/in/bertrandliard

With one of the largest and most experienced data privacy and cybersecurity groups in the world, White & Case's global team is on hand to guide clients through the relevant data protection legislation in the jurisdictions in which they are active. Seamlessly working with their counterparts in other practice areas, our global team has the depth of resources to provide integrated, creative and practical advice on the privacy-related concerns faced by our clients, wherever they are located. Our experience spans the full range of industry sectors including financial institutions and banking, biotechnology, pharmaceuticals and chemicals, construction and engineering, consumer goods and retail, automotive, hotels and leisure, IT, telecommunications, internet and social media, manufacturing and electronics, publishing and media.

www.whitecase.com



Germany



Martin Röleke



Dr. Evelyne Sørensen

activeMind.legal Rechtsanwaltsgesellschaft mbH

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The principal data protection legislation in the European Union (EU) and Germany is the General Data Protection Regulation¹ (GDPR), since 2018.

The GDPR aims to create a uniform level of data protection in all EU Members States, yet it does contain so-called “opening clauses” that allow EU Member States to legislate more specific regulations in certain areas in their respective jurisdiction.

1.2 Is there any other general legislation that impacts data protection?

Germany has made use of these “opening clauses” in its national data protection law, the Federal Data Protection Act² (BDSG). The BDSG contains more specific national regulations, especially regarding the processing of personal data in the employment context.

Data protection in Germany on a national level is thus governed by the GDPR, together with the more specific regulations contained in the BDSG.

1.3 Is there any sector-specific legislation that impacts data protection?

Electronic communication: The ePrivacy Directive³ has been implemented into national law in Germany by the *Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei digitalen Diensten* (TDDDG). Please refer to Section 11 (Cookies) for more information.

Marketing: The EU Unfair Commercial Practices Directive⁴ has been implemented in Germany by means of the Act against Unfair Competition⁵ (UWG). Please refer to Section 10 (Marketing) for more information.

Hospitals: Each federal state in Germany has published its own federal law governing hospitals in the state, so-called “Landeskrankenhausgesetze”, some of these contain specific data protection regulations.

1.4 What authority(ies) are responsible for data protection?

In Germany, each federal state has its own supervisory authority for data protection which is responsible for monitoring the application of the GDPR and the BDSG and the federal laws by public and private bodies.

In addition, the German Federal Commissioner for Data Protection and Freedom of Information is the supervisory authority for all federal public and semi-public bodies, e.g. postal service providers.

To ensure that this multitude of supervisory authorities has a uniform approach, a committee consisting of all authorities has been established – the Data Protection Conference (DSK). This body publishes guidance and coordinates actions.

Lastly, there are sector-specific supervisory authorities. The DSK maintains a list⁶ of all supervisory authorities.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

The definitions set out in Art. 4 GDPR⁷ and Art. 9 GDPR⁸ apply in Germany.

Art. 4 GDPR⁹ sets out the definitions of, e.g. “data subject”, “controller”, “processor”, “personal data” and “processing”.

Art. 9 GDPR sets out the categories of personal data that are generally referred to as “special categories of personal data” or “sensitive data”.

3 Territorial and Material Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The BDSG applies to private bodies if:

1. the private body, acting either as a controller or processor, processes personal data in Germany;
2. personal data are processed in the context of the activities of an establishment of the controller or processor in Germany; or
3. although the controller or processor has no establishment in the EU or the European Economic Area (EEA), it

does fall within the scope of the GDPR – this will be the case if Art. 3 (2) GDPR¹⁰ applies.

In terms of Art. 3 (2) GDPR, the GDPR will apply to a business if it is processing personal data stemming from the offering of free or paid goods or services to data subjects in the EU or the monitoring of behaviour of data subjects as far as their behaviour takes place in the EU.

If a business is offering free or paid goods or services to data subjects in Germany or is monitoring the behaviour of data subjects in the Germany, the BDSG and the GDPR shall apply.

3.2 Do the data protection laws in your jurisdiction carve out certain processing activities from their material scope?

The GDPR explicitly excludes any activity performed by a natural person in the course of a purely personal or household activity from its scope.

The BDSG provides national-level specifications on certain provisions of the GDPR but does not alter its material scope in a way that would conflict with the GDPR's broad applicability.

However, the BDSG does carve out specific exceptions and supplementary rules that refine the GDPR's application in Germany, particularly in areas where the GDPR allows for national discretion.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

In accordance with Art. 5 GDPR¹¹ and the BDSG, all processing of personal data must respect the following key principles:

- **Fairness**
The principle of fairness requires that any processing of personal data be in line with the reasonable expectations of the data subjects whose personal data is being processed.
- **Transparency**
Personal data shall be processed in a transparent manner in relation to the data subject. This includes informing and explaining to the data subject what data will be processed, how their data will be processed, for what purposes it will be processed and what rights they have in terms of their data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
- **Lawfulness**
Processing of any type of personal data is generally prohibited in the EU and in Germany; it is lawful only if and to the extent that a legal basis listed in Art. 6 GDPR¹² applies. For private bodies, the following legal bases are relevant:
 1. the data subject has given consent to the processing of his or her personal data for one or more specific purposes, such consent meeting the conditions of Art. 7 GDPR;¹³
 2. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
 3. processing is necessary for compliance with a legal obligation to which the controller is subject, and the

legal obligation comes from EU law, or a Member State law to which the controller is subject; and

4. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

The processing of special categories of personal data is further restricted. It is only permitted if one of the legal bases listed in Art. 9 GDPR or Sec. 22 BDSG¹⁴ apply. Sec. 26 BDSG¹⁵ sets out when processing of personal data may be lawful for employment-related purposes.

- **Purpose limitation**
Personal data must be collected for specified, explicit and legitimate purposes. It must not be processed further in a manner which is incompatible with these purposes. Where a private body intends to further process the personal data for a purpose other than that for which the personal data were collected, the private body shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information in terms of the transparency principle. This obligation is restricted in certain instances – see the “right to be informed” at question 5.1 below.
Sec. 24 BDSG¹⁶ further permits private bodies to process personal data for a purpose other than the one for which the data was collected. This is permitted if the processing is either necessary for (1) prevention of threats to public security, (2) prosecution of criminal offences, or (3) the establishment, exercise or defence of legal claims. However, this is permitted only if data subjects do not have an overriding interest in not having the data processed.
- **Data minimisation**
Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- **Accuracy**
Private bodies must ensure that the personal data they process is accurate and, where necessary, kept up to date. Reasonable steps must be taken to ensure that inaccurate personal data is erased or rectified without delay.
- **Storage limitation**
Personal data must not be kept in a form that permits identification of data subjects for longer than is necessary for the purposes for which the personal data are processed. Depending on the purposes for processing personal data, there may often be statutory retention deadlines that apply. In Germany, the applicable statutory retention deadlines are set out in various laws.
- **Integrity and confidentiality**
Personal data must be processed in a manner that ensures an appropriate level of security. In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing.
- **Accountability**
Every company is responsible for GDPR compliance and must always be able to demonstrate compliance with the above-mentioned principles when processing personal data. To fulfil this principle, documentation of all measures is thus required.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

The most important rights that individuals have in relation to the processing of their personal data arise directly from the GDPR.

These rights may be restricted on the basis of Art. 23 GDPR.¹⁷ In Germany, the BDSG provides for further restrictions of the respective rights.

■ Right to be informed

In line with the transparency principle, data subjects have the right to be informed about the processing of their personal data, even when their personal data is not collected directly from them. The information must be in accordance with Art. 13 GDPR¹⁸ and/or Art. 14 GDPR.¹⁹ If a private body processes personal data further for additional purposes aside from the original one, the right is further restricted in Germany by Sec. 32 BDSG²⁰ and Sec. 33 BDSG.²¹

■ Right of access to (copies of) data/information about processing

Data subjects have the right to obtain confirmation as to whether personal data concerning them are being processed, and, where that is the case, access to the personal data and the information listed in Art. 15 GDPR.²²

Additionally, the private body must provide a copy of the personal data being processed.

The right to access is restricted in Germany by the BDSG in certain instances; for private bodies the relevant restrictions are in Sec. 29 BDSG,²³ Sec. 27(2) BDSG,²⁴ Sec. 28(2) BDSG²⁵ and Sec. 34 BDSG.²⁶

■ Right to rectification

Data subjects have the right to rectification of inaccurate personal data and completion of incomplete data.

■ Right to deletion/right to be forgotten

Data subjects have the right to erasure of their personal data (the “right to be forgotten”) and private bodies are obligated to erase personal data if:

- the data subject withdraws consent on which the processing is based, and where there is no other legal ground for the processing;
- the data subject objects to the processing and there are no overriding legitimate grounds for the processing;
- the personal data have been unlawfully processed;
- the personal data have to be erased for compliance with a legal obligation in EU or Member State law to which the private body is subject; or
- the personal data is that of a child.

The right to deletion is restricted in Germany by Sec. 35 BDSG.²⁷

■ Right to object to processing

Data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data where the basis for that processing is the legitimate interest of the private body. The private body must cease such processing unless it demonstrates compelling legitimate grounds for the processing that override the interests, rights and freedoms of the relevant data subject or requires the data in order to establish, exercise or defend legal rights.

■ Right to restrict processing

Data subjects have the right to restrict the processing of personal data, which means that the data may only be held by the private body, and may only be used for limited purposes if: (i) the accuracy of the data is contested (and only for as long as it takes to verify that accuracy); (ii) the processing is unlawful and the data subject requests restriction (as opposed to exercising the right to erasure); (iii) the private body no longer needs the data for their original purpose, but the data are still required by the private body to establish, exercise or defend legal rights; or (iv) verification of overriding grounds is pending, in the context of an erasure request.

■ Right to data portability

Data subjects have a right to receive a copy of their personal data in a commonly used machine-readable format, and transfer their personal data from one private body to another or have the data transmitted directly between private bodies.

■ Right to withdraw consent

A data subject has the right to withdraw their consent at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject must be informed of the right to withdraw consent. It must be as easy to withdraw consent as it is to give it.

■ Right to object to marketing

Data subjects have the right to object to the processing of personal data for the purpose of direct marketing, including profiling.

■ Right protecting against solely automated decision-making and profiling

Data subjects have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects that concern (or similarly significantly affect) them. This right is restricted where the solely automated decision: (i) is necessary for entering into, or the performance of, a contract between the data subject and controller; (ii) is authorised by EU or Member State law to which the controller is subject (and which contains suitable measures to safeguard the data subject’s rights); or (iii) is based on the data subject’s explicit consent.

In addition to the restriction in the GDPR, the right is restricted in Germany by Sec. 37 BDSG.²⁸

■ Right to complain to the relevant data protection authority(ies)

Data subjects have the right to lodge complaints concerning the processing of their personal data at one of the German supervisory authorities, if the data subjects live in in Germany or the alleged infringement occurred in Germany.

■ Right to compensation

Data subjects who have suffered (material or non-material) damage as a result of the unlawful processing of their personal data have the right to receive compensation from the controller and/or processor for the harm suffered.

5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

The data subject shall have the right to mandate not-for-profit organisations that: have been properly constituted in

accordance with the law of Germany; have statutory objectives that are in the public interest; and are active in the field of the protection of data subjects' rights and freedoms, to seek remedies on their behalf or seek collective redress.

6 Children's Personal Data

6.1 What additional obligations apply to the processing of children's personal data?

Where information society services are offered directly to a child under the age of 16, and the lawful basis of processing their personal data is consent, such consent must be obtained from or authorised by the individual(s) with parental responsibility over the child. The controller must make reasonable efforts to verify that consent has been given, or authorised, by the holder(s) of parental responsibility in light of available technology.

Where personal data is collected and processed for purposes other than the provision of information society services, German national law applies. German law demands a case-by-case assessment; however, in practice, it is safe to say that a child over the age of 16 can give valid consent.

Given that children merit specific protection, any information and communication where processing is addressed to a child, should be in a clear and plain language that the child can easily understand.

7 Registration Formalities and Prior Approval

7.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

In Germany, there is no such legal obligation on businesses. Indirectly, businesses may be forced to do so if they are required to appoint a Data Protection Officer (**DPO**) due to the specific processing activities they undertake and to notify the data protection authority thereof. See below for more information.

7.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

This is not applicable in Germany.

7.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

This is not applicable in Germany.

7.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

This is not applicable in Germany.

7.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

This is not applicable in Germany.

7.6 What are the sanctions for failure to register/notify where required?

This is not applicable in Germany.

7.7 What is the fee per registration/notification (if applicable)?

This is not applicable in Germany.

7.8 How frequently must registrations/notifications be renewed (if applicable)?

This is not applicable in Germany.

7.9 Is any prior approval required from the data protection regulator?

This is not applicable in Germany.

7.10 Can the registration/notification be completed online?

This is not applicable in Germany.

7.11 Is there a publicly available list of completed registrations/notifications?

This is not applicable in Germany.

7.12 How long does a typical registration/notification process take?

This is not applicable in Germany.

8 Appointment of a Data Protection Officer

8.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The appointment of a DPO for private bodies in Germany, whether acting as controllers or processors, is mandatory in the following circumstances:

- their core activities consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale;
- their core activities consist of processing on a large scale of special categories of data pursuant to Art. 9 GDPR

and personal data relating to criminal convictions and offences referred to in Art. 10 GDPR;²⁹

- they constantly employ as a rule at least 20 persons dealing with the automated processing of personal data;
- they undertake processing subject to a Data Protection Impact Assessment (DPIA); or
- they commercially process personal data for the purpose of transfer, anonymised transfer, or market or opinion research.

For the latter, it is irrelevant how many persons are employed.

8.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

In the circumstances where appointment of a DPO is mandatory, failure to comply may result in administrative fines up to €10 million, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

8.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

If the appointment of a DPO is mandatory under the BDSG, the appointed DPO can only be dismissed or penalised for performing their tasks in accordance with strict requirements (see Sec. 626 BGB)³⁰ and not within a year following the end of their appointment. The DPO should report directly to the highest management level of the controller or processor.

8.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

A single DPO is permitted by a group of undertakings provided that the DPO is easily accessible from each establishment and the DPO is registered with each supervisory authority responsible for each of the entities.

8.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The DPO should be appointed on the basis of professional qualities and should have an expert knowledge of data protection law and practices.

8.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

The GDPR outlines the minimum tasks required by a DPO, which include: (i) informing the controller, processor and their relevant employees who process data of their obligations under the GDPR; (ii) monitoring compliance with the GDPR, national data protection legislation and internal policies in relation to the processing of personal data, including internal audits; (iii) advising on DPIAs and the training of staff; and (iv) co-operating with the data protection authority and acting as the authority's primary contact point for issues related to data processing.

In Germany, Sec. 6 BDSG³¹ additionally binds the DPO to maintain secrecy concerning the identity of data subjects and

concerning circumstances enabling data subjects to be identified, unless they are released from this obligation by the data subject.

8.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

Yes, the controller or processor must notify the data protection authority of the contact details of the designated DPO. This applies for every establishment individually if a group of undertakings appoints a single DPO.

8.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

When collecting personal data from a data subject or informing them that their data has been obtained from another source, controllers must provide the contact details of the DPO, if one has been appointed. This information is typically included in a privacy notice. Due to this requirement, the DPO will be named in a public-facing privacy notice.

9 Appointment of Processors

9.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes. Businesses intending to appoint a data processor to take on the processing of personal data on behalf of the business must conclude a contract, in practice called a data processing agreement (DPA), or ensure the processing is otherwise governed by a legal act under the EU or Member State law.

The GDPR imposes several key requirements that must be addressed in a DPA to ensure compliance. Therefore, the DPA should explicitly regulate all relevant provisions in accordance with GDPR standards. It is essential to ensure that the contractual terms align with the obligations set out in the regulation, covering aspects such as data security, breach notifications and data subject rights. See below for more information.

9.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The processor must be appointed under a binding agreement in writing (or electronically). The contractual terms must stipulate that the processor: (i) only acts on the documented instructions of the controller; (ii) imposes confidentiality obligations on all employees; (iii) ensures the security of personal data that it processes; (iv) abides by the rules regarding the appointment of sub-processors; (v) implements measures to assist the controller with guaranteeing the rights of data subjects; (vi) assists the controller in obtaining approval from the relevant data protection authority; (vii) either returns or destroys the personal data at the end of the relationship (except as required by EU or Member State law); and (viii) provides the controller with all information necessary to demonstrate compliance with the GDPR.

10 Marketing

10.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

The sending of electronic direct marketing messages is regulated by the UWG in Germany.

As a rule, to lawfully send electronic direct marketing messages, the recipient must have given prior, informed consent.

An exception to this rule is possible if there is (i) an existing contractual relationship with the recipient, i.e. the recipient has previously purchased a product or service, (ii) only products or services are marketed that are similar to the product or service already purchased, (iii) the recipient has not objected to the receipt of electronic marketing messages, (iv) the recipient was clearly informed at the time of collection of their personal data of the intended marketing and their right to object, and (v) the recipient is informed of their right to object and how to do so in every electronic marketing message received.

If electronic direct marketing is permissible under the UWG, the processing of the recipient's personal data for this purpose may be justified based on legitimate interest under Art. 6(1)(f) GDPR.

10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

The restrictions on electronic direct marketing also apply in the business-to-business context.

10.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

In contrast to electronic direct marketing, telephone marketing in terms of the UWG does differentiate between consumers (B2C) and other market participants (B2B). If consumers (B2C) are the intended recipients, prior, express consent is required, whereas if other market participants (B2B) are the recipients, so-called presumed consent may be sufficient.

Insofar as a recipient has not objected to the receipt of postal marketing, e.g. by covering their mailbox with a "no marketing" sticker, marketing by post is permitted.

Marketing conducted in person is not subject to any restrictions.

10.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?

The above restrictions also apply to marketing sent from other countries. The UWG applies to all marketing in Germany.

10.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

It is possible to lodge a complaint with a data protection authority about the unlawful processing of personal data for marketing purposes. If a marketing activity is prohibited by the UWG, one may not process personal data for this unlawful marketing activity either. The data protection authority will not enforce a breach of the marketing restrictions, but rather the consequent breach of the data protection laws.

10.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

The sale and purchase of marketing lists is not unlawful *per se*. However, under data protection law, there must be a legal basis for collecting and processing personal data for marketing purposes, the data subject must have been informed of the processing, and must, in most cases, have consented. When purchasing marketing lists, it is difficult to ensure all data protection requirements have been fulfilled.

10.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Breaches of data protection law arising from breaches of marketing restrictions can be subject to the highest penalties in terms of the GDPR and BDSG.

Under the UWG, businesses engaging in unsolicited marketing emails, SMS, or calls without prior consent can face fines of up to €50,000. For larger companies with an annual turnover exceeding €1.25 million, penalties can reach 4% of their annual revenue, with a maximum fine of €2 million if turnover is undetermined.

In severe cases, fraudulent or deceptive marketing practices can result in criminal liability, with penalties including imprisonment of up to two years or fines pursuant to the UWG.

11 Cookies

11.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

The TDDDG requires prior consent in terms of Art. 7 GDPR³² before the storage of cookies (or other data) on an end user's device may be permissible. This does not apply if: (i) the cookie is for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or (ii) the cookie is strictly necessary to provide an "information society service" (e.g. a service over the internet) requested by the subscriber or user, which means that it must be essential to fulfil their request.

11.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

Generally, cookies are either (i) technically necessary cookies which may be set without the consent of the end user, and

instead based on legitimate interest, or (ii) technically unnecessary cookies which always require the consent of the user and include, e.g. analytics cookies, marketing cookies and statistics cookies.

11.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

Yes. German supervisory authorities have taken enforcement action against breaches of the GDPR and BDSG based on breaches of the TDDDG.

11.4 What are the maximum penalties for breaches of applicable cookie restrictions?

Breaches of data protection law arising from breaches of cookie restrictions can be subject to the highest penalties in terms of the GDPR and BDSG. Breaches of the TDDDG can result in fines up to €300,000.

12 Restrictions on International Data Transfers

12.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Data transfers to other jurisdictions that are not within the EEA can only take place if the transfer is to an “Adequate Jurisdiction” (as specified by the EU Commission),³³ the business has implemented one of the required safeguards as specified by Art. 46 GDPR³⁴ or one of the derogations specified in Art. 49 GDPR³⁵ applies to the relevant transfer. Preference should be given to the safeguards provided for in the GDPR before relying on a derogation.

12.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

When transferring personal data to a country other than an Adequate Jurisdiction, businesses must ensure that there are appropriate safeguards on the data transfer, as prescribed by the GDPR. The GDPR offers a number of ways to ensure compliance for international data transfers, of which one is consent of the relevant data subject. Other common options are the use of Standard Contractual Clauses³⁶ (SCCs) or Binding Corporate Rules (BCRs).

Businesses can adopt the SCCs drafted by the EU Commission. International data transfers may also take place on the basis of contracts agreed between the data exporter and data importer provided that they conform to the protections outlined in the GDPR, and they have prior approval by the relevant data protection authority.

International data transfers within a group of businesses can be safeguarded by the implementation of BCRs. The BCRs will always need approval from the relevant data protection authority. Most importantly, the BCRs will need to include a mechanism to ensure they are legally binding and enforced by every member in the group of businesses. Among other

things, the BCRs must set out the group structure of the businesses, the proposed data transfers and their purpose, the rights of data subjects, the mechanisms that will be implemented to ensure compliance with the GDPR and the relevant complainant procedures.

Transfers of personal data to the US are possible on the basis of an adequacy decision if the data importer has signed up to the EU–US Data Privacy Framework³⁷ (DPF). The DSK has issued instructions on how to use the DPF.³⁸

12.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

Individual transfers to other jurisdictions do not require registration/notification or prior approval from the relevant data protection authority. However, some of the safeguards outlined in the GDPR used for making the transfers will need prior approval from the data protection authority.

12.4 Do transfers of personal data to other jurisdictions require a transfer impact assessment? If conducting a transfer impact assessment is only mandatory in some circumstances, please identify those circumstances.

In *Schrems II* (Case C-311/18), the Court of Justice of the EU clarified that controllers and processors exporting personal data from the EU must verify – on a case-by-case basis – whether the law and regulatory landscape of the recipient country ensure adequate protection to the personal data to be transferred. Prior to transferring personal data to a recipient in a jurisdiction that has not received an adequacy decision from the European Commission, the data exporter must undertake a transfer impact assessment to analyse whether the protection afforded to the transferred personal data by the laws of the third country needs to be supplemented by additional measures to ensure a level protection that is at least equivalent to that within the EEA.

12.5 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?

The European Data Protection Board has issued Recommendations 01/2020³⁹ on supplementary protections to be implemented where appropriate, in respect of transfers made under SCCs, in light of the *Schrems II* decision. These Recommendations are designed to assist data exporters with the task of assessing the laws of third countries and identifying appropriate measures to implement where the level of protection afforded to personal data is not essentially equivalent to that within the EEA.

12.6 What guidance (if any) has/have the data protection authority(ies) issued in relation to the use of standard contractual/model clauses as a mechanism for international data transfers?

The new SCCs published by the European Commission on 4

June 2021 (2021 SCCs) are to be used for international transfers. They have become the most popular form of safeguard for third country transfers if an adequacy decision cannot be relied upon. The European Commission issued an FAQ⁴⁰ regarding the 2021 SCCs which provides more guidance.

13 Whistle-blower Hotlines

13.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

Germany has implemented the EU Whistleblowing Directive⁴¹ in the German Whistleblower Protection Act. Anyone who qualifies as an employee may report to a whistleblowing channel. The channels must receive and investigate all reports of criminal offences, infringements that are subject to a fine if the violated regulation serves to protect life, limb or health or the protection of employees or their representative bodies, and a number of selected regulations, e.g. antitrust law, environmental law, radiation protection, food and product safety, anti-money laundering, consumer protection and data protection law.

13.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Businesses are free to decide whether to offer the option of anonymous reporting in Germany.

Irrespective of this, the identity of the whistleblower and the persons affected by the report are subject to special protection. In principle, the identity may only be disclosed to employees who are specifically responsible for handling the report. Exceptions apply, for example, if the report is the subject of a criminal investigation.

In Germany, businesses tend to offer the option of anonymous reporting.

14 CCTV

14.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

No, the use of CCTV does not require separate registration/notification or prior approval from the relevant data protection authority. Rather, if the planned CCTV meets the threshold, the controller may have to perform a DPIA and may have to inform the relevant data protection authority depending on the outcome of the DPIA. The DSK has issued guidance regarding video surveillance for non-public entities⁴² and has indicated that it believes a DPIA is only required for CCTV if systematic and extensive monitoring of publicly accessible areas takes place, or biometric procedures are used for data processing.

Regardless of whether CCTV requires a DPIA, the DSK recommends putting up a high-visibility sign informing about the CCTV and providing an additional extensive privacy policy.

14.2 Are there limits on the purposes for which CCTV data may be used?

The DSK makes it clear that CCTV may only be used for a legitimate purpose and identifies the following as legitimate purposes for use of CCTV: to protect against break-ins, theft, vandalism (property protection) or assaults (personal protection).

15 Employee Monitoring

15.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Sec. 26 BDSG in conjunction with the GDPR governs the processing of personal data in the employment context in Germany.

Sec. 26 BDSG requires that any employee monitoring be necessary for the performance or termination of the employment contract or consent and be proportional. In practice, in order to conduct employee monitoring, an individual assessment must be made in each case. To date, there are no clear guidelines.

15.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Consent may be a possible legal basis; however, in the employment context, it must be given formally and voluntarily. The latter is often questionable due to the inherent power imbalance between employer and employee.

Sec. 26 BDSG provides examples where employee consent is presumed to be voluntary, such as when the employee receives a legal or economic advantage by giving consent or has similar interests to the employer.

Before processing personal data, employers must obtain valid consent from employees, ensuring that it is informed and provided either electronically or in writing. In practice, employers often seek consent during the employee onboarding process.

15.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

In Germany, works councils must be notified any time employee data is impacted by a planned processing activity.

15.4 Are employers entitled to process information on an employee's attendance in office (e.g., to monitor compliance with any internal return-to-office policies)?

Yes, the decision of the European Court of Justice (ECJ) in Case C-55/18⁴³ established that employers are obligated under EU law to record employees' working hours in a structured, reliable manner. This requirement was subsequently confirmed by the German Federal Labour Court (*Bundesarbeitsgericht*, BAG) in its ruling (Case 1 ABR 22/21).⁴⁴ Accordingly, in Germany, the processing of employee data for time recording is lawful under Art. 6(1)(b) GDPR in conjunction with Sec. 26(1) BDSG, as it is necessary for the performance of the employment relationship.

The ECJ states that in the ruling: *"It follows that in the absence of a system enabling the time worked each day by each worker to be*

*measured there is nothing to ensure, as is clear moreover from the elements provided by the referring court referred to in paragraph 26 above, that actual compliance with the right to a limitation on maximum working time and minimum rest periods conferred by Directive 2003/88 is fully guaranteed to workers, since that compliance is left to the discretion of the employee... The Member States must require employers to set up an objective, reliable and accessible system enabling the duration of time worked each day by each worker to be measured.*⁷⁴⁵

16 Data Security and Data Breach

16.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Yes. Personal data must be processed in a way that ensures security and safeguards against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, controllers and processors must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

16.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

The controller is responsible for reporting a personal data breach without undue delay (and in any case within 72 hours of first becoming aware of the breach) to the relevant data protection authority, unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject(s). A processor must notify any data breach to the controller without undue delay.

The notification must include the nature of the personal data breach, including the categories and number of data subjects concerned, the name and contact details of the DPO or relevant point of contact, the likely consequences of the breach and the measures taken to address the breach, including attempts to mitigate possible adverse effects.

16.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Controllers have a legal requirement to communicate the breach to the data subject, without undue delay, if the breach is likely to result in a high risk to the rights and freedoms of the data subject.

The notification must include the name and contact details of the DPO (or point of contact), the likely consequences of the breach and any measures taken to remedy or mitigate the breach.

The controller may be exempt from notifying the data subject if the risk of harm is remote (e.g. because the affected data is encrypted), the controller has taken measures to minimise the risk of harm (e.g. suspending affected accounts) or the notification requires a disproportionate effort (e.g. a public notice of the breach).

16.4 What are the maximum penalties for personal data security breaches?

The maximum penalty is the higher of €20 million or 4% of worldwide turnover.

17 Enforcement and Sanctions

17.1 Describe the enforcement powers of the data protection authority(ies).

- (a) **Investigative powers:** The data protection authority has wide powers to order the controller and the processor to provide any information it requires for the performance of its tasks, to conduct investigations in the form of data protection audits, to carry out review on certificates issued pursuant to the GDPR, to notify the controller or processor of alleged infringement of the GDPR, to access all personal data and all information necessary for the performance of controllers' or processors' tasks and access to the premises of the data, including any data processing equipment. No criminal sanctions apply.
- (b) **Corrective powers:** The data protection authority has a wide range of powers, including to issue warnings or reprimands for non-compliance, to order the controller to disclose a personal data breach to the data subject, to impose a permanent or temporary ban on processing, to withdraw a certification and to impose an administrative fine (as below). No criminal sanctions apply.
- (c) **Authorisation and advisory powers:** The data protection authority has a wide range of powers to advise the controller, accredit certification bodies and to authorise certificates, contractual clauses, administrative arrangements and BCRs as outlined in the GDPR. No criminal sanctions apply.
- (d) **Imposition of administrative fines for infringements of specified legal provisions:** The GDPR provides for administrative fines which can be €20 million or up to 4% of the business's worldwide annual turnover of the preceding financial year. No criminal sanctions apply.
- (e) **Non-compliance with a data protection authority:** The GDPR provides for administrative fines, which will be €20 million or up to 4% of the business's worldwide annual turnover of the preceding financial year, whichever is higher. No criminal sanctions apply.

17.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The GDPR entitles the relevant data protection authority to impose a temporary or definitive limitation, including a ban on processing.

17.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

The data protection authorities in Germany focus on larger companies that are particularly risky.

17.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

The German data protection authorities rarely exercise their powers against businesses established outside Germany. Enforcement depends on whether the business is established in another EU country or the EEA, and whether there are treaties in place to provide for assistance with enforcement.

18 E-discovery/Disclosure to Foreign Law Enforcement Agencies

18.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Businesses in Germany typically review any such legitimate requests for compliance with data protection laws, especially whether a legal basis for a transfer of personal data exists, whether a cross-border transfer is permitted in terms of data protection law and whether there are sufficient technical and organisational measures in place.

18.2 What guidance has/have the data protection authority(ies) issued on disclosure of personal data to foreign law enforcement or governmental bodies?

The German data protection authorities have not issued guidance on this topic.

19 Artificial Intelligence

19.1 Are there any limitations on automated decision-making involving the processing of personal data using artificial intelligence?

In Germany, automated decision-making using Artificial Intelligence (AI) is subject to strict regulations under both the GDPR and BDSG.

According to Art. 22 GDPR,⁴⁶ individuals have the right not to be subject to fully automated decisions that significantly affect them, such as in credit scoring, hiring or insurance assessments. Such decisions are only allowed if: (i) they are explicitly authorised by law; (ii) they are necessary for fulfilling a contract; or (iii) the individual has given explicit consent. Additionally, affected individuals have the right to human intervention, to express their views and to challenge decisions. Organisations must ensure transparency by explaining the logic behind the AI decision.

Sec. 37 BDSG⁴⁷ complements Art. GDPR by specifying when automated decision-making is lawful. It permits such decisions that are made in the context of providing services pursuant to an insurance contract if:

- the data subject's request is fully granted; or

- the decision follows binding reimbursement rules for therapeutic treatment and the insurer takes the following suitable measures:
 - (a) ensures human intervention upon request;
 - (b) allows the data subject to express their opinion and contest the decision; and
 - (c) informs them of these rights when denying or partially granting the request.

Under Sec. 31 BDSG,⁴⁸ AI-based credit scoring and risk assessment models must: (i) be based on statistically sound methods; (ii) use relevant and verifiable data; and (iii) ensure that decisions are not solely automated and allow for human review. This provision primarily applies to financial institutions and credit agencies, ensuring fairness in credit-scoring decisions.

19.2 What guidance (if any) has/have the data protection authority(ies) issued in relation to the processing of personal data in connection with artificial intelligence?

In Germany, the DSK, the collective body of federal and state data protection authorities, has issued comprehensive guidance on the processing of personal data in connection with AI. On 6 May 2024, the DSK released the document titled "Artificial Intelligence and Data Protection",⁴⁹ aiming to ensure that AI applications comply with the GDPR.

In addition, since Germany has multiple data protection authorities, various guidelines have been published by different authorities.

In January 2024, the Bavarian Data Protection Authority released guidelines on AI and data protection, expanding its information offerings to address the application of the GDPR and other legal requirements in the context of AI technologies.⁵⁰

The Hamburg Data Protection Authority issued a checklist for the use of Large Language Model-based chatbots, providing practical guidance on ensuring GDPR compliance when deploying such AI applications.⁵¹

The Baden-Württemberg Data Protection Authority published a paper on legal bases in data protection for the use of AI, offering insights into establishing lawful grounds for AI-related data processing activities.⁵²

20 Trends and Developments

20.1 In your opinion, what enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.

Germany's various data protection authorities cannot be said to focus on specific types of violations, specific industry sectors or adhere to enforcement trends.

In 2024, Germany's Federal Court of Justice (BGH) issued a landmark decision on data protection law,⁵³ ruling that losing control over personal data constitutes non-material damage under the GDPR, allowing compensation claims without proving additional harm. The court established criteria for assessing damages, significantly lowering the threshold for individuals seeking compensation and increasing accountability for data controllers.

In its decision of 5 March 2024 (VI ZR 330/21),⁵⁴ the BGH clarified the scope of the right to obtain copies under Art. 15(3) GDPR. The court held that individuals are entitled to receive full copies of documents they themselves sent to the data controller, even if they already have them. However, for documents created by the

controller, only the parts containing the individual's personal data must be disclosed – not the full document. The ruling provides important guidance on balancing transparency with proportionality in data-access requests.

In its judgment of 19 December 2024 (Case C65/23),⁵⁵ the ECJ clarified that employee data processing based on collective or works agreements must still comply with the GDPR's core principles. The ECJ emphasised that such agreements cannot override GDPR safeguards, and that national courts must verify whether the agreed data processing is genuinely necessary and proportionate. This decision reinforces the importance of GDPR compliance – even within internal workplace arrangements. Accordingly, the decision makes clear that even where Sec. 26 BDSG permits data processing on the basis of collective agreements, such processing must still comply fully with the requirements of the GDPR – particularly the principles of lawfulness, necessity and proportionality as set out in Arts 5 and 6.

20.2 In your opinion, what “hot topics” are currently a focus for the data protection regulator?

With the introduction of the AI Act and rapid advancements in AI technologies, the intersection of AI and data protection law has become a key focus. As companies and regulators strive to adapt to these emerging technologies while ensuring compliance, the fast-paced evolution of AI presents ongoing challenges in keeping up with regulatory and industry trends.

The European Health Data Space (EHDS) regulation will enter into force on 26 March 2025. The EHDS is a key part of the European Health Union, aiming to create a common framework for the use and exchange of electronic health data across the EU. It enhances individuals' access to and control over their health data and allows certain data to be reused for public interest, policy support and research. The EHDS fosters a single market for digital health services and products and establishes a harmonised framework for electronic health record systems. European regulators intend to provide a trustworthy setting for secure access to and processing a wide range of health data. Therefore, the EHDS builds on key existing horizontal EU frameworks, including the GDPR, Data Governance Act, Data Act and Network and Information Systems Directive.

Endnotes

- 1 <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- 2 https://www.gesetze-im-internet.de/englisch_bdsgr
- 3 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02002L0058-20091219>
- 4 <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX%3A32005L0029%3Aen%3AHTML>
- 5 https://www.gesetze-im-internet.de/englisch_uwgr
- 6 <https://www.datenschutzkonferenz-online.de/datenschutzaufsichtsbehoerden.html>
- 7 <https://www.activemind.legal/legislation/gdpr/article-4>
- 8 <https://www.activemind.legal/legislation/gdpr/article-9>
- 9 <https://www.activemind.legal/legislation/gdpr/article-4>
- 10 <https://www.activemind.legal/legislation/gdpr/article-3>
- 11 <https://www.activemind.legal/legislation/gdpr/article-5>
- 12 <https://www.activemind.legal/legislation/gdpr/article-6>
- 13 <https://www.activemind.legal/legislation/gdpr/article-7>
- 14 <https://www.activemind.legal/legislation/fdpa/paragraph-22>
- 15 <https://www.activemind.legal/legislation/fdpa/paragraph-26>
- 16 <https://www.activemind.legal/legislation/fdpa/paragraph-24>
- 17 <https://www.activemind.legal/legislation/gdpr/article-23>
- 18 <https://www.activemind.legal/legislation/gdpr/article-13>
- 19 <https://www.activemind.legal/legislation/gdpr/article-14>
- 20 <https://www.activemind.legal/legislation/fdpa/paragraph-32>
- 21 <https://www.activemind.legal/legislation/fdpa/paragraph-33>
- 22 <https://www.activemind.legal/legislation/gdpr/article-15>
- 23 <https://www.activemind.legal/legislation/fdpa/paragraph-29>
- 24 <https://www.activemind.legal/legislation/fdpa/paragraph-27>
- 25 <https://www.activemind.legal/legislation/fdpa/paragraph-28>
- 26 <https://www.activemind.legal/legislation/fdpa/paragraph-34>
- 27 <https://www.activemind.legal/legislation/fdpa/paragraph-35>
- 28 <https://www.activemind.legal/legislation/fdpa/paragraph-37>
- 29 <https://www.activemind.legal/legislation/gdpr/article-10>
- 30 https://www.gesetze-im-internet.de/bgb/_626.html
- 31 <https://www.activemind.legal/legislation/fdpa/paragraph-6>
- 32 <https://www.activemind.legal/legislation/gdpr/article-7>
- 33 https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
- 34 <https://www.activemind.legal/legislation/gdpr/article-46>
- 35 <https://www.activemind.legal/legislation/gdpr/article-49>
- 36 https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en
- 37 <https://www.dataprivacyframework.gov/list>
- 38 https://www.datenschutzkonferenz-online.de/media/ah/230904_DSK_Ah_EU_US.pdf
- 39 https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en
- 40 https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en
- 41 <https://eur-lex.europa.eu/eli/dir/2019/1937/oj>
- 42 https://www.datenschutzkonferenz-online.de/media/oh/20200903_oh_v%C3%BC_dsk.pdf
- 43 Court of Justice of the European Union (ECJ), Judgment of 14 May 2019, Case C55/18 – *Federación de Servicios de Comisiones Obreras (CCOO) v Deutsche Bank SAE*, ECLI:EU:C:2019:402. Available at: <https://curia.europa.eu/juris/document/document.jsf?docid=214043&doclang=EN>
- 44 Federal Labour Court (*Bundesarbeitsgericht* – BAG), Decision of 13 September 2022, Case 1 ABR 22/21. Available at: <https://www.bundesarbeitsgericht.de/entscheidung/1-abr-22-21>
- 45 ECJ, Judgment of 14 May 2019, Case C55/18 – *Federación de Servicios de Comisiones Obreras (CCOO) v Deutsche Bank SAE*, ECLI:EU:C:2019:402, paras. 58, 60. Available at: <https://curia.europa.eu/juris/document/document.jsf?docid=214043&doclang=EN>
- 46 <https://www.activemind.legal/legislation/gdpr/article-22>
- 47 <https://www.activemind.legal/legislation/fdpa/paragraph-37>
- 48 <https://www.activemind.legal/legislation/fdpa/paragraph-31>
- 49 https://www.datenschutzkonferenz-online.de/media/oh/20200903_oh_v%C3%BC_dsk.pdf
- 50 https://www.datenschutzkonferenz-online.de/media/oh/20200903_oh_v%C3%BC_dsk.pdf

- 51 https://www.datenschutzkonferenz-online.de/media/oh/20200903_oh_v%C3%BC_dsk.pdf
- 52 https://www.datenschutzkonferenz-online.de/media/oh/20200903_oh_v%C3%BC_dsk.pdf
- 53 <https://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2024&nr=139818&linked=urt&Blank=1&file=dokument.pdf>
- 54 Federal Court of Justice (BGH), Judgment of 5 March 2024, Case No. VI ZR 330/21. Available at: <https://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&Datum=Aktuell&Sort=12288&nr=137175&pos=16&anz=1340>
- 55 <https://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2024&nr=139818&linked=urt&Blank=1&file=dokument.pdf>



Martin Röleke advises national and international corporations across all industries in the areas of data protection and information security law at activeMind.legal.

His consulting focus lies, in particular, on the interface of data protection and IT security. He primarily advises on various data protection compliance requirements in the area of health care, where he provides support for research and complex outsourcing projects.

activeMind.legal Rechtsanwaltsgesellschaft mbH

Potsdamer Str. 3
80802 Munich
Germany

Tel: +49 89 919 294 900

Email: roeleke@activemind.legal

LinkedIn: www.linkedin.com/in/martin-r%C3%B6leke



Dr. Evelyn Sørensen specialises in national and international data protection law and is partner at activeMind.legal. She supports clients across all industries.

Her area of expertise is, in particular, the legal support of national and international corporations in the introduction and development of new (digital) business models. In addition to complex data protection issues such as the structuring of international data flows, she supports clients in privacy by design, as well as in the context of data protection breaches. Another focus is on advising companies on Swiss data protection law.

activeMind.legal Rechtsanwaltsgesellschaft mbH

Potsdamer Str. 3
80802 Munich
Germany

Tel: +49 89 919 294 900

Email: soerensen@activemind.legal

LinkedIn: www.linkedin.com/in/dr-evelyne-j-b-sørensen-ll-m-a19326

activeMind.legal is a specialised law firm in Germany and the United Kingdom. We advise on both the European data protection regime and the United Kingdom data protection regime, utilising resources familiar with both jurisdictions and fluent in the languages.

Our lawyers and consultants have years of experience advising companies, organisations and authorities from many industries and fields of work on data protection and information security issues. Our experts are equipped with extensive legal, technical and organisational knowledge and training. Additionally: We speak more than 10 European languages!

www.activemind.legal

activeMind.legal

Greece



Dr. Nikos Th. Nikolinakos



Dina Th. Kouvelou



Alexis N. Spyropoulos

Nikolinakos & Partners Law Firm

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

Since 25 May 2018, the principal data protection legislation in the EU has been Regulation (EU) 2016/679 (the General Data Protection Regulation or GDPR). The GDPR repealed Directive 95/46/EC (Data Protection Directive) and has led to increased (though not total) harmonisation of data protection law across the EU Member States.

Since 29 August 2019, the main data protection legislation in Greece has been Law 4624/2019, which has implemented the GDPR and incorporated Directive (EU) 2016/680. Law 4624/2019 repealed previous Law 2472/1997, which incorporated Directive 95/46/EC.

1.2 Is there any other general legislation that impacts data protection?

- Law 3471/2006, which incorporates Directive 2002/58/EC (the ePrivacy Directive) – as amended by Directive 2006/13/EC – is complementary and specific to the institutional framework for the protection of personal data in the field of electronic communications.
- Law 5169/2025 ratified the Amending Protocol of 10/10/2018 to the Council of Europe’s Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

1.3 Is there any sector-specific legislation that impacts data protection?

Data protection provisions are further dispersed across various Greek laws:

- Law 5002/2022 on the procedure for lifting the confidentiality of communications, cybersecurity and protection of personal data of citizens.
- Law 4990/2022 on the protection of persons reporting breaches of EU law and incorporation of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 and other urgent arrangements.
- Law 4961/2022 on emerging information and communication technologies, strengthening digital governance and other provisions.
- Law 4579/2018 sets obligations on air operators regarding passengers’ details.

- Law 4577/2018, transposing the NIS Directive (EU 2016/1148), imposes obligations for system and network security on businesses in the fields of energy, transport, credit, financial infrastructure, health, water and digital infrastructure, e-commerce and information society services.
- Law 3917/2011 regulates the retention of data that is produced or processed based on the provision of publicly available electronic communication services or public communication networks and the use of audio or video surveillance systems in public spaces.
- Law 3783/2009 establishes the framework for the collection and storage of identification data of mobile services subscribers for national security purposes and for the identification of particularly serious crimes.
- Article 8 of Law 3144/2003 introduces requirements for the processing of workers’ medical data.

1.4 What authority(ies) are responsible for data protection?

The Hellenic Data Protection Authority (HDPa) is a constitutionally established independent public authority that serves as the watchdog for the application and enforcement of the data protection legislation.

Moreover, the Hellenic Authority for Communication Security and Privacy (ADAE) is responsible for the protection of free correspondence and communication, including personal data issues in telecommunications.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **“Personal Data”**
Any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- **“Processing”**
Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording,

organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

- **“Controller”**

The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

- **“Processor”**

A natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.

- **“Data Subject”**

An individual who is the subject of the relevant personal data.

- **“Sensitive Personal Data”/“Special Categories of Personal Data”**

Personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or sex life and sexual orientation, genetic data or biometric data.

- **“Data Breach”**

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

- **“Profiling”**

Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

- **“Pseudonymisation”**

The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

- **“Filing system”**

Any structured set of personal data which is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

- **“Recipient”**

A natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.

- **“Consent”**

Any freely given, specific for the purposes of the case, unambiguous and informed indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

- **“Public body”**

Public authorities, independent and regulatory administrative authorities, legal persons governed by public law, first- and second-level local authorities and their legal persons and undertakings, State or public undertakings and bodies, legal persons governed by private law

owned or subsidised by the State by at least 50% of their annual budget or whose administration is appointed by the State.

- **“Private body”**

A natural or legal person or an association of persons without legal personality, which does not fall within the concept of “public body”.

3 Territorial and Material Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The GDPR applies to businesses established in any EU Member State that process personal data (either as Controllers or as Processors, regardless of whether the processing takes place in the EU or not) in the context of that establishment.

A business that is not established in any Member State but is subject to the laws of a Member State by virtue of public international law is also subject to the GDPR.

The GDPR applies to businesses outside the EU if they (either as Controllers or Processors) process the personal data of EU residents in relation to: (i) the offering of goods or services (whether or not in return for payment) to EU residents; or (ii) the monitoring of the behaviour of EU residents (to the extent that such behaviour takes place in the EU).

Further, the GDPR applies to businesses established outside the EU if they monitor the behaviour of EU residents (to the extent such behaviour takes place in the EU).

3.2 Do the data protection laws in your jurisdiction carve out certain processing activities from their material scope?

The GDPR expressly excludes certain activities from its scope. In particular, processing carried out in the course of an activity that falls outside the scope of EU law, activities performed by Greece concerning the common foreign and security policy of the EU or processing carried out by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security that are outside the material scope of the GDPR. Similarly, the processing of personal data by a natural person in the course of a purely personal or household activity is exempted from the material scope of the GDPR.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**

Personal data must be processed lawfully, fairly and in a transparent manner.

- **Lawful basis for processing**

The GDPR provides an exhaustive list of legal bases on which personal data may be processed, of which the following are the most relevant for businesses: (i) prior, freely given, specific, informed and unambiguous consent of the data subject; (ii) contractual necessity; (iii) compliance with the Controller’s legal obligations;

or (iv) the Controller's legitimate interests, except where they are overridden by the interests, fundamental rights or freedoms of the data subjects.

The processing of sensitive personal data is only permitted under certain conditions, of which the most relevant for businesses are: (i) explicit consent provided by the data subject; (ii) the processing is necessary under employment law provisions; (iii) the processing is necessary for the establishment, exercise or defence of legal claims; or (iv) the data have already been disclosed publicly.

■ **Purpose limitation**

Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with them. If a Controller wishes to use the relevant personal data in a manner that is incompatible with the initial purposes, the data subject must be informed beforehand; and a lawful basis of processing must be provided.

■ **Data minimisation**

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed.

■ **Proportionality**

Only the personal data which is adequate and relevant for the purposes of the processing is collected and processed.

■ **Retention**

Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be retained for longer periods of time if they have been stored, for the purposes of scientific or historical research or for statistical purposes in the public's interest and provided that the appropriate technical and organisational measures are applied.

■ **Accuracy**

Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that inaccurate personal data are erased or rectified without delay.

■ **Data security**

Personal data must be processed in a manner that ensures their security, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage.

■ **Accountability**

The Controller is responsible for, and must be able to demonstrate compliance with, the data protection principles.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

■ **Right of access to (copies of) data/information about processing**

Data subjects have the right to obtain from Controllers information regarding: (i) the purposes and the location of the processing; (ii) the categories of data being processed; (iii) the categories of recipients with whom the data may be shared; (iv) the period for which the data will be stored; (v) the existence of the rights to erasure, rectification, restriction of processing and to object to processing; (vi) the existence of the right to complain to

the relevant data protection authority; (vii) the source of the data, if they have not been collected from the data subject; and (viii) the existence of, and an explanation of the logic involved in any automated processing that has a significant effect on the data subject.

Access to data may be denied when the exceptions provided in Article 33 of Law 4624/2019 are applicable. Upon request, a copy of the personal data being processed can be provided to the data subject.

■ **Right to rectification of errors**

Data subjects have the right to have inaccurate or incomplete personal data erased, rectified or completed.

■ **Right to deletion/right to be forgotten**

Data subjects have this right in situations where: (i) the data are no longer needed for their original purpose; (ii) the data subject has withdrawn its consent for processing, and no other lawful ground exists; (iii) the data subject exercises the right to object, and the Controller has no overriding grounds for continuing the processing; (iv) the data have been processed unlawfully; or (v) erasure is necessary for compliance with EU or national data protection law. Article 17 GDPR provides a list of exceptions, where the data subjects are refused the deletion of their data. Additionally, Article 33 of Law 4624/2019 stipulates that if certain conditions are met, the deletion of the data may be replaced by the mere restriction of their processing.

■ **Right to object to processing**

Data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data where the basis for that processing is either in the public interest or the legitimate interest of the Controller. The Controller must cease such processing unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or requires the data in order to establish, exercise or defend legal rights. Law 4624/2019 stipulates that the right to object does not apply in cases involving public bodies or when data processing is conducted for scientific, historical research, or statistical purposes, subject to specific conditions being met.

■ **Right to restrict processing**

The right to restrict processing means that the data may only be held by the Controller, and may only be used for limited purposes if: (i) the accuracy of the data is contested (and only for as long as it takes to verify that accuracy); (ii) the processing is unlawful and the data subject requests restriction; (iii) the Controller no longer needs the data for their original purpose, but the data are still required by the Controller to establish, exercise or defend legal rights; or (iv) verification of overriding grounds is pending, in the context of an erasure request. If the restriction is lifted at any point, the Controller is required to inform the data subject.

■ **Right to data portability**

Data subjects have a right to receive a copy of their personal data in a commonly used machine-readable format and transfer their personal data from one Controller to another or have the data transmitted directly between Controllers.

■ **Right to withdraw consent**

Data subjects may withdraw their consent at any time. This withdrawal does not affect the lawfulness of processing based on consent before its withdrawal. Prior

to giving consent, the data subject must be informed of this right. It must be as easy to withdraw consent as to give it.

■ **Right to object to marketing**

Data subjects have the right to object to the processing of personal data for the purpose of direct marketing, including profiling.

■ **Right protecting against solely automated decision-making and profiling**

Data subjects have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects that concern (or similarly significantly affect) them. This right is restricted where the solely automated decision: (i) is necessary for entering into, or the performance of, a contract between the data subject and Controller; (ii) is authorised by EU or Member State law to which the Controller is subject (and which contains suitable measures to safeguard the data subject's rights); or (iii) is based on the data subject's explicit consent.

■ **Right to complain to the relevant data protection authority(ies)**

Data subjects have the right to lodge complaints concerning the processing of their personal data with the HDPa if the data subjects live in Greece or the alleged infringement occurred in Greece.

■ **Right to basic information**

Data subjects have the right to be provided with information relating to the processing in a concise, transparent, intelligible and easily accessible form.

■ **Right to compensation**

Data subjects who have suffered (material or non-material) damage as a result of an infringement of the GDPR have the right to receive compensation from the Controller or Processor for the harm suffered.

5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

Data subjects have the right to mandate not-for-profit organisations that: (i) have been properly constituted in accordance with the law of Greece; (ii) have statutory objectives that are in the public interest; and (iii) are active in the field of the protection of data subjects' rights and freedoms, to represent the data subject in the submission of a complaint before the HDPa, as well as in any court action against the HDPa, pursuant to Article 41 of Law 4624/2019. The possibility of not-for-profit organisations representing a data subject in seeking remedies against a Controller or Processor is not provided for in Greek law.

6 Children's Personal Data

6.1 What additional obligations apply to the processing of children's personal data?

Where information society services are offered directly to a child under the age of 16, and the lawful basis of processing their personal data is consent; such consent must be obtained from or authorised by the legal representative of the child. The Controller must make reasonable efforts to verify that consent has been given, or authorised, by the holder of parental responsibility in light of available technology. Member States

may provide by law for a lower age limit for these purposes, provided that such age limit is not below 13 years of age.

Greek Law 4624/2019 has lowered the minimum age for the above purposes. Specifically, according to Article 21, the direct provision of information society services to minors based on their consent is lawful only if they are over 15 years of age. If they are under 15 years of age, such processing is lawful only after obtaining consent from their legal representative.

Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in a clear and plain language that the child can easily understand. The Controller must ensure that the child is informed and understands what they are consenting to, otherwise the consent is invalid.

Automated decision-making is, in principle, prohibited if these decisions may have a legal effect on children or may affect them significantly. The GDPR gives children the right not to be subject to such decisions and while exceptions to this right exist, they only apply if appropriate measures have been taken to protect the rights, freedoms and interests of the child.

Additionally, in case a profile is created for children, the Controller should provide clear information regarding the processing of their data, while profiling for marketing purposes is prohibited. The Controller must respect the absolute right of the child to oppose actions relating to direct marketing and to cease such actions as soon as requested.

7 Registration Formalities and Prior Approval

7.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

Businesses are not required to register or notify the HDPa or any other governmental body in respect of their processing activities. They are, however, required to request a prior consultation with the HDPa pursuant to Article 36(1) GDPR, in situations where a data protection impact assessment (DPIA) has indicated that processing activities result in a high risk that the Controller cannot mitigate by implementing appropriate measures. Therefore, a prior consultation with the HDPa is required whenever the Controller cannot identify adequate measures to reduce the risks to an acceptable level.

Controllers may submit a prior consultation request to the HDPa provided that they have verified that the necessary formality criteria ensuring the completeness of the DPIA based on Article 35 (2) and (7)–(9) GDPR and the Guidelines on Data Protection Impact Assessments of the European Data Protection Board (EDPB) relating to the request for consultation are met.

The request for a consultation must include at least a detailed description of the residual high risks and their potential consequences, as well as a detailed documentation of the reasons for which measures to reduce the high risk to an acceptable level cannot be adopted. The request must also have the DPIA attached to it and include the elements set out in Article 36(3) GDPR.

The request for prior consultation is submitted electronically, through the online portal of the HDPa and in exceptional cases via email.

Where the HDPa is of the opinion that the intended processing would infringe the GDPR, it shall, within a period of up to eight weeks after receiving the request, provide written

advice to the Controller and/or Processor. That period may be extended by six weeks, taking into account the complexity of the intended processing. The time limits may be suspended until the supervisory authority has obtained the information it has requested for the purposes of the consultation.

7.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

This is not applicable to Greece.

7.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

This is not applicable to Greece.

7.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

This is not applicable to Greece.

7.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

This is not applicable to Greece.

7.6 What are the sanctions for failure to register/notify where required?

This is not applicable to Greece.

7.7 What is the fee per registration/notification (if applicable)?

This is not applicable to Greece.

7.8 How frequently must registrations/notifications be renewed (if applicable)?

This is not applicable to Greece.

7.9 Is any prior approval required from the data protection regulator?

This is not applicable to Greece.

7.10 Can the registration/notification be completed online?

This is not applicable to Greece.

7.11 Is there a publicly available list of completed registrations/notifications?

This is not applicable to Greece.

7.12 How long does a typical registration/notification process take?

This is not applicable to Greece.

8 Appointment of a Data Protection Officer

8.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The appointment of a Data Protection Officer (DPO) for Controllers or Processors is mandatory where: (i) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (ii) the core activities of the Controller or the Processor consist of processing that requires regular and systematic large-scale monitoring of data subjects; and/or (iii) the core activities of the Controller or Processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences. The mandatory appointment of a DPO for public authorities is also provided in Article 6 of Greek Law 4624/2019.

Businesses are free to appoint a DPO despite not being legally obliged to do so.

In situations where a business or organisation designates a DPO on a voluntary basis, the relevant requirements of the GDPR concerning their designation, position and tasks apply as if the designation had been mandatory.

8.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

In cases where the appointment of a DPO is mandatory, failure to comply may result in a fine of up to €10 million by the HDPA, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

8.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

The appointed DPO should not be dismissed or penalised by the Controller or Processor for performing their tasks and should report directly to the highest management level of the organisation.

8.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

A group of undertakings may appoint a single DPO, provided that the DPO is easily accessible from each establishment.

8.5 Please describe any specific qualifications for the Data Protection Officer required by law.

DPOs should be appointed based on professional qualities, have an expert knowledge of data protection law and practices, and be able to fulfil the tasks referred to in Article 39 GDPR (see question 8.6 below). It follows that the knowledge and level of skills required will vary depending on the complexity of the processing conducted by each business.

8.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

The DPO supports organisations in achieving and maintaining compliance with the GDPR while also acting as a mediator between the various stakeholders. The GDPR specifies that at a minimum, the DPO must: (i) inform the Controller or the Processor and any employees carrying out processing activities of their responsibilities under the data protection legislation; (ii) monitor the organisation's compliance with the GDPR and other EU or Greek data protection provisions and the policies adopted by the organisations themselves in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits; (iii) provide advice concerning the DPIA and monitor its performance; (iv) cooperate with the HDPA; and (v) act as the contact point for the HDPA. It should be noted that the role of the DPO is advisory and not decisive.

8.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

Yes, the Controller or Processor must notify the HDPA of the contact details of the designated DPO. The notification is carried out through the online portal of the HDPA or, in exceptional cases, via email.

8.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

The DPO does not necessarily need to be named in the public-facing privacy notice. However, the Controller or the Processor must publish the contact details of the DPO to ensure unhindered communication with data subjects. The contact details must also be notified to the data subject when personal data relating to that data subject are collected.

9 Appointment of Processors

9.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes, where processing is to be carried out on behalf of a Controller, the Controller and Processor are required to enter into a contract or other legal act that is binding on the Processor with regard to the Controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the Controller.

9.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The agreement between the Controller and Processor must be in writing and, in accordance with Article 28 GDPR, must stipulate that the Processor: (i) only acts on the documented instructions of the Controller; (ii) imposes confidentiality obligations on all employees; (iii) ensures the security of personal data that it processes; (iv) abides by the rules regarding the appointment of sub-processors; (v) implements measures to assist the Controller with guaranteeing the rights of data subjects; (vi) assists the Controller in obtaining approval from the relevant data protection authority; (vii) either returns or destroys the personal data at the end of the relationship (except as required by EU or Greek law); and (viii) provides the Controller with all information necessary to demonstrate compliance with the GDPR and allows for and contributes to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

10 Marketing

10.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

Electronic direct marketing requires the clear affirmative consent of the recipient, which must be consistent with the definition of consent and any further conditions set out in the GDPR. In the telecommunications sector, Law 3471/2006, which transposes the e-Privacy Directive into the Greek legal framework, stipulates in Article 11 that unsolicited direct marketing conducted through any means of electronic communications, with or without human intervention, is permitted only with the recipients' prior explicit consent. However, email addresses legitimately acquired in the context of a previous transaction may be used for marketing purposes even without the recipient's consent, on condition that the recipient is provided with the clear option to opt out, at the stage of collection and in every subsequent communication.

Direct marketing emails or messages must state the identity of the sender or advertiser and a manner (e.g. a specific email address, pursuant to Law 3471/2006) through which recipients may opt out from receiving further communications. Sending emails that do not contain the necessary information required for marketing communications or encourage their recipients to visit webpages that violate Article 11 of Law 3471/2006 is prohibited. Law 3471/2006 also establishes the rules that apply in case consent is given by electronic means. In particular, the Controller must ensure that users or subscribers act in full knowledge of the consequences of their statement, which is also recorded in a secure manner, is accessible to the user or subscriber at all times and may at any time be withdrawn. The HDPA has adopted Directive 2/2011, which contains best practices for obtaining consent by electronic means for direct marketing purposes. According to this Directive, Controllers must implement opt-in confirmation mechanisms adapted to the specific electronic medium used, e.g. email, SMS, phone call, etc. Finally, in the case of marketing emails concerning goods or services, the sender is obliged to indicate the commercial nature of the content in the subject of the message, according to Presidential Decree 131/2003.

10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

The restrictions concerning personal data apply only to the data of individuals and not legal entities. However, information identifying sole traders may constitute personal data and restrictions may also apply to marketing addressed to employees in their business emails. The restrictions of Article 11 of Law 3471/2006 outlined above apply also to legal entities and therefore in a business-to-business context.

10.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

Directive 50/2000 of the HDPA outlines the mandatory requirements which apply to marketing by post. Specifically, in order to lawfully send printed promotional material through the post:

- (i) The recipient must have consented to receiving promotional material.
- (ii) If the recipient has not provided their consent, the Controller may send promotional material if all the following conditions are met:
 - The data has been collected from public directories, or the data subjects themselves have made it for related purposes, or on the basis of the customer relationship or transactional contact.
 - The data is limited to what is strictly necessary to achieve the specific purpose. Where the data is not collected from the data subjects, only their name, address and occupation may be considered necessary data.
 - The Controller has consulted the Register of persons that do not wish to be included in lists intended to promote goods or services at a distance. Persons in this register must be removed from the Controller's lists used for the above purposes.
 - The Controller enables the exercise of the right to object directly to the Controller and excludes persons who have expressed their objection from any future promotional action.
 - When sending promotional material, the Controller provides recipients with the information in Article 14 GDPR, including the source from which the data were collected, making it clear that it is an advertisement or action aimed at promoting sales of goods or services, and to enable recipients to exclude their personal data from any further use for the above purpose.

Telephone marketing calls with human intervention, according to Article 11 of Law 3471/2006, are permitted unless the individual has previously opted out of receiving such calls, up to 30 days before the call is made. This opt-out system applies both to the advertiser's clients and to persons whose data is drawn from a public directory of subscribers. To opt out, individuals or legal persons may object to the processing of their data either specifically to the advertiser (the Controller), who must retain a record of such objections, or generally by registering to the relevant registry of subscribers kept by each public telecommunications service provider. Article 11 of

Law 3471/2006 provides for the creation of opt-out registers by each telecommunications service provider, which are kept publicly and can be accessed by anyone interested in using them for direct marketing. The HDPA, taking into account the objective difficulty of collecting and processing registers from all providers, has held that advertisers must obtain updated copies of Article 11 registers from all providers and make sure that they retain subscribers' updated statements made up to 30 days before the telephone call is made. In addition to the above, when making promotional calls with human intervention, the advertiser must ensure that its employees state the details of the Controller and any Processor, as well as information on the exercise of the right to access and the right to object.

10.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?

The GDPR applies to organisations that are based in the EU even if the data is stored or processed outside of the EU, and also to organisations that are not in the EU if one of the conditions for extraterritorial application set in the GDPR apply. On the contrary, Law 3471/2006 does not have formal extraterritoriality provisions.

10.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

The HDPA is active in the enforcement of marketing restrictions, with recent examples being: the imposition of a monetary fine on an undertaking for the illegal use of client data for marketing purposes; failure to satisfy a data subject's right to object to the processing; and its recent assessment of several complaints concerning unsolicited marketing telephone calls, for which it imposed sanctions.

In its most recent decision, the HDPA examined several repeated complaints against a matchmaking agency regarding unsolicited communication via short text messages (SMS). Taking into account the number of violations, in total 15, out of a total of the same number of complaints, regarding unsolicited communication in the field of electronic communications, as well as a previous decision against the specific Controller and the non-cooperation of the Controller with the HDPA, the HDPA imposed a fine of €45,000 on the Controller for established violations of Articles 11 of Law 3471/2006 and 31 GDPR.

10.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Purchasing marketing lists from third parties is lawful under the condition that the obtaining organisation is able to demonstrate that the data was obtained in compliance with the GDPR and that it can use it for advertising purposes, as well as to ensure that the list is kept up to date and that individuals who have objected to the processing of their personal data for direct marketing purposes are not sent any marketing communications. The obtaining organisation must also inform data subjects, at the latest when sending them the initial communication, that it has collected their personal data and that it will be processing it for the above purposes.

10.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

The GDPR and Law 4624/2019 provide the HDPa with different options in case of non-compliance with the data protection rules such as warnings (in case of potential infringement) or reprimands, temporary or permanent ban of processing and/or fines up to €20 million (in case of actual infringement). According to Law 3471/2006, the fines for breaching the above-mentioned restrictions can amount to up to €150,000. Other penalties provided include warnings, provisional or temporary removal of licences, the destruction of the records or the cessation of processing activities and the destruction, return or freezing of the data, as well as the payment of full compensation and compensation for moral damage, by a natural or legal entity, which, in violation of Law 3471/2006, causes material damage. In fact, the monetary compensation for moral damage is set at a minimum at the amount of €10,000, unless a smaller amount is requested by the plaintiff.

11 Cookies

11.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

The installation and use of “cookies” are regulated by paragraph 5 of Article 4 of Law 3471/2006. The following cases are exceptions to the above obligation: (i) the sole purpose of the cookie is carrying out the transmission of a communication over an electronic communications network; or (ii) the cookie is strictly necessary to provide an “information society service” requested by the subscriber or user, meaning that it is essential to fulfil their request. The basic principle is that the installation and use of cookies is permitted only with the user’s prior consent. For consent to be valid, it should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject’s agreement to the processing of their personal data. The HDPa issued its Recommendations 1/2020, which provided clarification regarding the best and worst practices on cookies, especially concerning the obligation and the way of obtaining the user’s consent, as well as the way and the content of the necessary information.

On February 11, 2025, the European Commission disclosed in the “2025 Work Programme” that it will withdraw the proposal for a new ePrivacy Regulation (replacing the current ePrivacy Directive). The withdrawal means that the current ePrivacy Directive and its national transposition laws will remain in force.

11.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

Yes, the applicable restrictions distinguish between different types of cookies. There are two types of cookies, those which require the user’s consent and those which do not. The first category includes the necessary cookies, which are considered technically necessary: (a) for the identification and/or retention of content entered by the subscriber or user during a session on a website throughout the specific connection; (b) to connect the subscriber or user to services that require authentication for user security to perform the technique of load

distribution (load balancing) on a link to a website; and (c) to maintain the user’s choices regarding the presentation of the website. The second category of cookies includes cookies installed for online advertising, targeting, functionality and web analytics.

11.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

The HDPa conducted remote audits on Controllers’ websites, finding a significant lack of compliance with the specific requirements of electronic data processing legislation and the GDPR regarding the management of cookies and related technologies. However, the HDPa has not yet proceeded to any enforcement action.

11.4 What are the maximum penalties for breaches of applicable cookie restrictions?

In case of violation of the applicable cookie restrictions, a fine of up to 20% or up to 4% of the worldwide turnover may be imposed.

12 Restrictions on International Data Transfers

12.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Data transfers to jurisdictions that are not within the European Economic Area (EEA) can only take place if the transfer is made on the basis of an adequacy decision by the EU Commission, the business has implemented one of the required safeguards as specified by the GDPR, or one of the derogations specified in the GDPR applies to the relevant transfer. The EDPB Guidelines (2/2018) set out that a “layered approach” should be taken with respect to the transfer mechanisms, meaning that adequacy decisions are preferred as the legal basis of the international data transfer. If the transfer is not covered by an adequacy decision, the data exporter should first explore the possibility of implementing one of the safeguards provided in the GDPR before relying on a derogation under Article 49. Moreover, the EDPB has issued Guidelines 2/2020 on Articles 46(2)(a) and 46(3)(b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies.

12.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

When transferring personal data to a country that is not covered by an adequacy decision, businesses must ensure that there are appropriate safeguards on the data transfer, as prescribed by the GDPR. The GDPR offers a number of ways to ensure compliance for international data transfers, such as the consent of the relevant data subject, Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs).

Businesses can adopt the SCCs drafted by the EU Commission, which are available for transfers between: (i) Controllers; (ii) Processors; (iii) a Controller (as exporter) and a Processor (as importer); and (iv) a Processor (as exporter) and a Controller (as importer). International data transfers may also take place on the basis of contracts agreed between the data exporter and data importer, provided that they conform to the protections outlined in the GDPR and they have prior approval by the relevant data protection authority.

International data transfers within a group of businesses can be safeguarded by the implementation of BCRs, the prior approval of which from the lead supervisory data protection authority is always required. Crucially, the BCRs need to include a mechanism to ensure they are legally binding and enforced by every member in the group of businesses, both internally and externally. Among other things, the BCRs must set out the group structure of the businesses, the proposed data transfers and their purpose, the rights of data subjects, the mechanisms that will be implemented to ensure compliance with the GDPR and the relevant complainant procedures.

On 10 July 2023, the EU Commission adopted a new adequacy decision concerning the US. Transfer of personal data to the US is now possible if the data importer has signed up to the EU-US Data Privacy Framework, which has been designed by the US Department of Commerce in consultation with the EU Commission to provide businesses in the EU and the US with a mechanism to comply with data protection requirements when transferring personal data from the EU to participating US companies and government agencies without the need to use any of the transfer tools provided for in Article 46 GDPR, nor to establish additional data protection safeguards through additional measures.

12.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

Prior authorisation from the HDPa is required in the following cases:

- (a) *Ad hoc* contractual clauses between the data importer and exporter.
- (b) Administrative arrangements between public authorities or bodies, which include enforceable and substantive rights of subjects (e.g., MoUs between public authorities with respective responsibilities). Permission of the HDPa is necessary because such administrative arrangements are legally non-binding.

Prior approval from the HDPa is required in the case of BCRs, on the condition that the HDPa is acting as the Lead Supervisory Authority (LSA). In this case, the draft of the BCRs must also be submitted to the HDPa in Greek.

In order to obtain the HDPa's relevant permission or submit the required notification, the data exporter should complete a special form and submit it electronically, through the HDPa's web portal or via email in exceptional cases.

There is no explicit provision for the time required for approval by the HDPa of the submitted applications, but in practice it takes approximately three months (e.g., HDPa Decision 2136/2019).

12.4 Do transfers of personal data to other jurisdictions require a transfer impact assessment? If conducting a transfer impact assessment is only mandatory in some circumstances, please identify those circumstances.

In *Schrems II* (Case C-311/18), the Court of Justice of the EU (CJEU) clarified that Controllers and Processors exporting personal data from the EU must verify – on a case-by-case basis – whether the law and regulatory landscape of the recipient country ensures adequate protection to the personal data to be transferred. Prior to transferring personal data to a recipient in a jurisdiction that has not received an adequacy decision from the EU Commission, the data exporter must conduct a transfer impact assessment to analyse whether the protection afforded to the transferred personal data by the laws of the third country needs to be supplemented by additional measures to ensure a level protection that is at least equivalent to that within the EEA. The requirement to carry out an assessment of the risks of the transfer of personal data outside the EEA is also provided in Section III of the new SCCs drafted by the EU Commission (“Local laws and practices affecting compliance with the Clauses”).

12.5 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?

The HDPa has not issued specific guidelines or recommendations pertaining to non-EU data transfers following *Schrems II*. However, the HDPa points to the EDPB's 2020 statement concerning the judgment and to the answers to the Frequently Asked Questions the EDPB has published on the judgment.

The EDPB has issued Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, in light of the *Schrems II* decision. These Recommendations are designed to assist data exporters in assessing the laws of third countries and identifying appropriate measures to implement where the level of protection afforded to personal data is not essentially equivalent to that within the EEA. Such protections include technical measures (e.g., pseudonymising personal data or encrypting it while in transit), contractual measures (e.g., certification by a data importer that it has not created any “back doors” that could be used to access the personal data or contractual provision for a “warrant canary” method) and organisational measures (e.g., ensuring adequate internal policies that contain clear allocation of responsibilities for data transfers or regular publication of transparency reports).

12.6 What guidance (if any) has/have the data protection authority(ies) issued in relation to the use of standard contractual/model clauses as a mechanism for international data transfers?

The new SCCs published by the European Commission on 4 June 2021 replaced the SCCs adopted under the Data Protection Directive.

According to the HDPa, the new SCCs reflect the requirements of the GDPR, as well as the conclusions reached by the CJEU in the *Schrems II* judgment and seek to ensure a high level of protection of personal data, taking into account the challenges faced by businesses in the digital age.

13 Whistle-blower Hotlines

13.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

Greek Law 4990/2022 transposes Directive (EU) 2019/1937 into national legislation, establishing a comprehensive framework for the protection of individuals who report breaches of EU law. The law mandates the creation of both internal and external reporting mechanisms and imposes corresponding obligations on public and private entities. These obligations include the organisation of procedures for submitting, receiving and monitoring reports, as well as the enforcement of sanctions for non-compliance. Organisations with 50 or more employees are required to appoint an Officer for the Receipt and Follow-up of Reports related to breaches within the law's scope. The law extends protection to whistle-blowers who report or disclose violations in various areas, including public procurement, financial services, anti-money laundering and counter-terrorism financing, transport safety, environmental protection, food and feed safety, public health, consumer rights, data privacy and cybersecurity. Regarding confidentiality, Greek Law 4990/2022 requires competent authorities to implement appropriate technical and organisational safeguards – such as pseudonymisation – when handling reports and communicating with relevant bodies. According to Article 14(3) of the law, unjustified failure to notify is considered a disciplinary offence for individuals subject to disciplinary procedures. Once a report is submitted, the whistleblower has the right to provide written comments to the authority managing the disclosure. These comments remain confidential. However, in exceptional cases where the authority deems the reasons insufficient, the disclosure of the whistleblower's identity and other confidential details may be permitted. Even in such cases, safeguards protecting the identity of the reporting person and related sensitive information remain in force, as stipulated by relevant EU and national legislation. The law covers individuals in both public and private sectors who have acquired information about violations in the course of their professional activities. This includes: current and former employees; self-employed individuals; shareholders; members of administrative, management or supervisory bodies; as well as contractors and suppliers. In implementation of the law, Joint Ministerial Decision 47312/2023 was issued to define the detailed procedure for submitting, receiving, managing and following up on internal reports within both public and private entities, while the issuance of a ministerial decision regarding the fines imposed in case of non-compliance is still pending.

13.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous reporting is not prohibited under EU data protection law; however, it poses certain challenges. Specifically, it can complicate compliance with the principle of fair data collection and hinder thorough investigations. Additionally, it limits the possibility of follow-up communication with the reporter if further clarification or information is needed. Despite these limitations, anonymous reports are processed in

the same manner as identified ones, with all legal procedures duly followed. Accordingly, Article 7, Paragraph 3 of Greek Law 4990/2022 provides legal protection to individuals who initially reported or disclosed breaches anonymously but were later identified and suffered retaliation. This protection applies if the conditions in Paragraph 1 of the same article are met – specifically, that at the time of reporting, the individual had reasonable grounds to believe the information was accurate and within the law's scope.

14 CCTV

14.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

In 2018, the HDPA issued a list of processing activities that require a DPIA. According to this list, a DPIA must be conducted by the Controllers, in cases of large-scale systematic processing for monitoring, observing or controlling natural persons using data collected through video surveillance systems over a public area, publicly accessible area or private area accessible to an unlimited number of persons. If the DPIA demonstrates that the residual risks remain high, the Controllers must consult the HDPA (see response to question 7.1). Regarding the required public notice of the operation of a CCTV, in its 2/2020 Recommendations, the HDPA provided model signs and documents to help Controllers comply with the requirement to provide information when processing data through video surveillance systems. Specifically, the HDPA has defined the content of the warning signs and its accompanied privacy notices, as well as the area where they must be placed in order to ensure that they are visible from all possible entry points into the monitored area.

14.2 Are there limits on the purposes for which CCTV data may be used?

In Directive 1/2011, the HDPA provided guidelines for the legal use of video surveillance systems in private areas accessible to the public. The Directive defined that the use of CCTV is permitted in order to protect persons and goods located in the monitored area based on the legitimate interest or the legal obligation of the administrator of the site in order to protect persons and property from unlawful acts. The same applies concerning the protection of health, safety, wellbeing and property of third parties that are lawfully present in the monitored area. The use of CCTV is also permitted for the provision of health services when the Controller is a healthcare provider, in cases where patients may cause harm to themselves or others or for monitoring patients in ICUs. Following the entry into force of the GDPR and Law 4624/2019, this Directive must be applied in conjunction with the provisions of the GDPR.

Personal data processing using CCTV in workplaces, whether publicly accessible or not, is only permitted if it is necessary for the protection of persons and goods. The HDPA has expressly stated that CCTV systems should not be used to monitor employees in order to evaluate or assess them or for training purposes.

For purposes other than the protection of persons and goods, which fall within the scope of the GDPR, Controllers must follow the general approach of assessing the lawfulness

of the processing, choosing an appropriate legal basis, satisfying the basic principles of legality, ensuring that the rights of data subjects are satisfied, etc. The lawfulness of such processing is assessed by the Controller on a case-by-case basis and properly documented with the accountability tools provided in the GDPR.

The HDPa, following the issuance of Presidential Decree 75/2020 on the use of CCTV and audio recording in public spaces for the purpose of preventing and suppressing specific criminal acts, regulating traffic, and preventing and managing road accidents, published its 3/2020 Opinion, making clear its opposition to several provisions.

15 Employee Monitoring

15.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Employee monitoring in Greece is permitted only under strict conditions, in accordance with the GDPR and Law 4624/2019. Any such monitoring must comply with the principles outlined in Articles 5 and 6 GDPR. According to Article 27 of Law 4624/2019, the processing of employees' personal data, including any form of monitoring, is permitted only when it is absolutely necessary either for the decision to enter into an employment contract or, following the conclusion of such contract, for its execution. The processing of special categories of personal data is also permitted if it is necessary for exercising rights or fulfilling obligations arising from labour, social security or social protection law, and provided there is no overriding interest on the part of the data subject. This also applies in cases where processing is not carried out within an archiving system.

Permitted types of monitoring include those strictly necessary for the operation and protection of the business, provided that no less intrusive means are available. This may include the below.

CCTV

The processing of personal data through CCTV systems within the workplace, whether publicly accessible or not, is permitted only if it is necessary for the protection of persons and property. The data collected through such systems may not be used as a criterion for evaluating employee performance. Employees must be informed in writing, either in physical or electronic form, regarding the installation and operation of the video surveillance system within the workplace.

Computer

An employer may access data stored on an employee's computer or monitor electronic communications only if such processing is strictly necessary to serve a legitimate interest, such as ensuring the smooth operation of the business, protecting confidential information or preventing serious threats, provided that this interest clearly outweighs the employee's rights and does not infringe upon their fundamental freedoms. To ensure the lawfulness of such monitoring, the employer must inform the employee in advance, in a clear and appropriate manner, about the monitoring methods, the purpose of the processing, and all necessary details for fair and transparent data handling, including a clear statement of the applicable monitoring policies and procedures.

GPS

The use of geolocation systems by employers is permitted under Greek data protection law only when it serves

legitimate purposes such as improving operational efficiency or ensuring employee safety, and not for monitoring employee behaviour. When used solely to assist employees (e.g., with navigation), the system must be limited to that purpose, with the employee retaining the right to deactivate it. Monitoring employee performance through such systems is generally considered disproportionate. For geolocation to be lawful, it must be limited to predefined routes during working hours, data retention must not exceed one month, appropriate security measures must be in place, pseudonymisation or encryption must be applied, employees must be fully informed about the processing and must have access to the data concerning them.

Electronic communications

In exercising its managerial right, and under the condition that the principles set out in Article 5(1) GDPR are respected, the employer, based on pre-established procedures and safeguards prior to the commencement of processing and within the framework of internal compliance in accordance with the principle of accountability, is entitled to monitor the electronic communication tools it provides to employees for the performance of their duties. Such processing must, in line with the principle of proportionality, be strictly necessary for the pursuit of the employer's legitimate interest and must clearly prevail over the rights and interests of the employee, without infringing upon their fundamental freedoms, as provided under Article 6(1)(f) GDPR. Prior to any such monitoring, employees must be informed accordingly and must be provided with an intelligible, clear and precise statement of the policy and procedures governing the monitoring of electronic communications.

Furthermore, the employer, acting as the Controller, must have drawn up and implemented an internal regulation governing the proper use and operation of the information and communication systems by employees, who are the data subjects. This regulation must be appropriately communicated to the employees.

Telephone communications

Telephone communications made from the workplace, including both their content and external details such as call duration and number dialled, are considered part of the employee's private life and are protected by data protection laws and the confidentiality of electronic communications. Any interference with this confidentiality is only allowed under strict legal safeguards.

These provisions apply to all individuals employed under any form of employment, service or project contract in both the public and private sectors, as well as to job applicants and former employees.

15.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Prior consent is not required if the processing is based on the employment contract. However, in cases where personal data processing is based, by exception, on the employee's consent, such consent must be freely given, taking into account the inherent dependency in the employment relationship and the circumstances under which consent was provided. This consent must be provided in written or electronic form, must be clearly distinguished from the employment contract, and must be accompanied by information on the purpose of processing and the employee's right to withdraw consent.

If the employer introduces a new form of monitoring, or makes significant changes to existing practices, the affected employees must be informed ahead of time. The notice must also be updated accordingly.

15.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

Greek legislation does not explicitly require prior consultation with works councils or employee representatives before the implementation of employee monitoring measures. However, it is strongly advisable that workers' representatives are informed in advance and given the opportunity to express their opinion, especially in cases involving intrusive monitoring methods such as CCTV surveillance or biometric systems.

15.4 Are employers entitled to process information on an employee's attendance in office (e.g., to monitor compliance with any internal return-to-office policies)?

Yes, employers are entitled to process information on an employee's attendance in office, including for the purpose of monitoring compliance with internal policies, such as return-to-office policies. Such processing is generally considered lawful when it is necessary for the purposes of the legitimate interests pursued by the employer, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject that require protection of personal data (Article 6(1)(f) GDPR).

That said, any such processing must still respect the principles of data minimisation, transparency and purpose limitation. The employer must, among others, clearly inform employees of the monitoring method, the legal basis and their rights (Article 13 GDPR). Several HDPA decisions reaffirm that attendance monitoring is permissible only during working hours, and only to the minimum extent necessary. Excessive or covert tracking will not be considered lawful, and any collected data must be retained only for as long as necessary to fulfil the stated purpose.

16 Data Security and Data Breach

16.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Personal data must be processed using technical and organisational measures meeting the requirements of the GDPR, in a way that ensures security and safeguards against unlawful processing. This obligation applies to both Controllers and Processors, who must ensure that they have the appropriate technical and organisational measures to meet the requirements of the GDPR, such as pseudonymisation and encryption, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, the ability to restore the availability and access to personal data in a timely manner, and the control of physical and logical access to personal data.

16.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

In the case of a personal data breach, the Controller must, without undue delay and no later than 72 hours after having become aware of it, notify the personal data breach to the HDPA, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of the natural persons. This obligation applies to the Processor as well, who must notify the Controller without undue delay after becoming aware of a personal data breach. The notification must contain specific information, such as the nature/extent of the incident, the categories of persons affected, the actions taken to address and mitigate the breach, etc.

16.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Controller must communicate the personal data breach to the data subject without undue delay, in accordance with Article 34 GDPR. According to Article 33(5) of Law 4624/2019, the above obligation shall not apply to the extent that the notification would entail the disclosure of information which, according to the law or by reason of its nature, in particular, due to overriding legitimate interests of third parties, should remain confidential.

16.4 What are the maximum penalties for personal data security breaches?

The HDPA may impose fines up to €10 million or 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher, or, for serious violations related to data subjects' rights, fines up to €20 million or 4% of the total worldwide annual turnover, whichever is higher. When the Processor is a public body, the fine can go up to €10 million.

17 Enforcement and Sanctions

17.1 Describe the enforcement powers of the data protection authority(ies).

- (a) **Investigative powers:** The HDPA conducts investigations and audits on compliance with the data protection legislation, requesting and receiving all information necessary for its tasks, and access to the premises and data processing equipment. It may also carry out reviews on certificates and notify the Controller/Processor of alleged infringements of the legislation.
- (b) **Corrective powers:** The HDPA issues warnings or reprimands for non-compliance, setting the manner or deadline to comply with, such as rectification or erasure of

personal data, destruction of filing systems, disclosure of data breaches to the subjects, limitation or ban on processing and withdrawal of certifications. It may also impose administrative fines.

- (c) **Authorisation and advisory powers:** The HDPa has the power to advise the Controller, issue opinions, guidelines and recommendations, approve codes of conduct or certification criteria, issue certificates, accredit certification bodies, authorise standard and contractual clauses, administrative arrangements and BCRs. The HDPa also advises data subjects, issues standard documents and complaint forms, and adopts regulatory acts for specific, technical and detailed matters.
- (d) **Imposition of administrative fines for infringements of specified legal provisions:** See response to question 17.3.
- (e) **Non-compliance with a data protection authority:** In cases of non-compliance with the HDPa's Directives or Decisions, the HDPa may impose fines on the Controller, which may be up to €20 million or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. If the Processor is a public body, the fine may amount to €10 million.

17.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

Yes. The HDPa has the power to impose temporary or permanent restrictions, including a ban on processing.

17.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

The HDPa examines complaints and holds hearings on infringements of the GDPR, basing its decisions on the nature, the gravity and the duration of the infringement, its impact on data subjects, the Controller's degree of liability, conduct and history, and the risk of repetition, among other factors. Acting within its corrective powers, the HDPa frequently imposes fines for infringements of the GDPR.

The HDPa, in a case regarding the lawfulness of the processing of voters' personal data by two members of a Greek political party, initially found the party liable as a Controller for violation of Article 25 GDPR (data protection by design) as it allowed the party members to process voters' personal data without supervision and guidance. The political party was fined €30,000 while it was also ordered to delete all data of overseas voters in its possession and to remedy deficiencies in data protection procedures. The HDPa also imposed a fine of €10,000 on the political party for violating the principle of lawfulness of processing, purpose limitation and the legal basis of legitimate interest. The party members, one of whom possessed the illegal material with the personal data of overseas voters and the other whom sent this file to a Greek member of the European Parliament, were fined €10,000 each for violating the principle of lawfulness of processing, purpose limitation and the legal basis of legitimate interest (HDPa Decision 38/2024).

The HDPa dealt with complaints against "Google LLC" for not satisfying the right of deletion of data. The HDPa found that the right of deletion must be satisfied and instructed "Google LLC" to immediately remove/delete the links that

arise as results based on the search criteria of the name of the complainant in the search engine. The HDPa issued enforcement orders for the violations of Articles 12(2) (3) and 37(7) GDPR and did not impose any administrative fines (HDPa Decision 54/2024).

Following a significant number of complaints filed against a Greek bank for violation of the right of access, the HDPa examined seven cases jointly and investigated the bank's procedures for ensuring timely and correct response to access requests. In all the cases examined, the HDPa found that the bank had exceeded the deadline for responding. In addition, the HDPa found that the bank lacked adequate procedures to ensure the proper and timely management of access requests, in particular after they grew in number due to the increasing fraud incidents, and that the bank's DPO had not contributed to compliance monitoring and updating the bank's procedures. In assessing compliance, the HDPa took into account the volume and nature of the personal data processed by the bank and the multiple access requests it is expected to receive due to its field of activity and the possible risks from the delay in the granting the right of access, as well as the bank's failure to identify the reasons behind its lack of compliance. The HDPa concluded by imposing on the bank a fine of €20,000 for violating Article 15(1) and (3) GDPR, a reprimand for violating Article 12(3) and (5) and Article 15 GDPR, as well as a fine of €200,000, for violating Articles 25(1) and 12(2) GDPR (HDPa Decision 1/2025).

After examining a number of repeated complaints against a dating agency regarding unsolicited communication through text messages, the HDPa imposed a fine of €45,000 on the agency-Controller for violations of Articles 11 of Law 3471/2006 and 31 GDPR, taking into account the number of violations, the fact that a previous Decision had been issued against the Controller, as well as the fact that the Controller had not cooperated with the HDPa (HDPa Decision 8/2025).

The HDPa also frequently issues opinions on draft laws, such as Opinion 2/2025 regarding a draft law on measures to implement Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 (Data Governance Act).

17.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

In cases of cross-border data processing, the cooperation mechanism between the LSA and the concerned supervisory authorities applies as a general rule. The primary responsibility for supervising the cross-border processing lies with the LSA.

The HDPa may act as an LSA for cross-border processing carried out by a controller or processor having its principal or sole establishment in Greek territory, in accordance with the procedure laid down in Article 60 GDPR. Where one of the conditions referred to in Article 4(22) GDPR is met, the HDPa acts as a concerned supervisory authority.

By derogation from the general rule, the HDPa competent to handle a complaint lodged with it or a possible infringement of the GDPR in cases where cross-border processing with local impact is carried out in Greek territory, if the LSA decides not to deal with the case after being informed by the HDPa. In such an event, the HDPa handles the case in accordance with Articles 61 and 62 GDPR.

18 E-discovery/Disclosure to Foreign Law Enforcement Agencies

18.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

E-discovery and disclosure requests are not part of the Greek legal framework. Such requests are assessed by businesses depending on their legal basis, their purpose and on the nature and type of information requested.

18.2 What guidance has/have the data protection authority(ies) issued on disclosure of personal data to foreign law enforcement or governmental bodies?

The HDPa has not issued such guidance yet.

19 Artificial Intelligence

19.1 Are there any limitations on automated decision-making involving the processing of personal data using artificial intelligence?

Under Article 22 GDPR, individuals have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them. This provision applies directly in Greece and is complemented by Law 4624/2019, which implements the GDPR at a national level.

For law enforcement purposes, Article 52 of Law 4624/2019 (transposing Article 11 of Directive 2016/680) provides that:

- Automated decision-making that produces adverse legal effects or significantly affects the data subject is prohibited, unless explicitly authorised by law with safeguards, including clear information, human intervention, justification of the decision, and rights to challenge or request review.
- Profiling that results in discrimination based on special categories of data (such as health or ethnic origin) is explicitly prohibited.

Additionally, under Article 35(3)(a) GDPR, a DPIA is mandatory where the processing involves systematic and extensive evaluation of personal aspects based on automated processing (including profiling) that produces legal or similarly significant effects. The HDPa has published a DPIA list that includes such cases.

19.2 What guidance (if any) has/have the data protection authority(ies) issued in relation to the processing of personal data in connection with artificial intelligence?

At the time of writing, the HDPa has not issued specific standalone guidelines exclusively dedicated to artificial intelligence (AI).

20 Trends and Developments

20.1 In your opinion, what enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.

Over the past 12 months, the HDPa has issued a number of Decisions and Opinions. Of them, the most noteworthy are the imposition of a fine and a compliance order on a Member of the European Parliament and the Ministry of Foreign Affairs following the leak of a personal data file of Greeks abroad (HDPa Decision 16/2024) in violation of Articles 5(1), 6(1), 14, 25, 32 and 33 GDPR. In the same case, the HDPa also imposed a fine on a Greek political party and two of its members (HDPa Decision 38/2024). In addition, the HDPa has imposed administrative fines on Controllers for violation of the rights of data subjects (mainly the right of access), while decisions have also been issued concerning illegal video surveillance either in homes or workplaces. In addition, a fine was imposed on a candidate MP-doctor of a public hospital for the use of patient data for the purpose of political communication.

20.2 In your opinion, what “hot topics” are currently a focus for the data protection regulator?

AI will be the primary focus of data protection regulators. As AI technologies are increasingly used in areas like recruitment, credit scoring and personalised services, regulators must ensure compliance with GDPR principles, particularly regarding automated decision-making and profiling. The use of AI raises concerns about fairness, accuracy and bias in decision-making processes. Ensuring that AI systems respect individuals' rights and provide transparency, as well as human intervention when needed, is crucial to safeguarding personal data in this rapidly evolving field.



Dr. Nikos Th. Nikolinakos is the Managing Partner of Nikolinakos & Partners Law Firm. He features prominently in the TMT, Data Protection, Cybersecurity, Tech Disputes, Competition Law and Intellectual Property rankings of leading Bar publications. Nikos divides his specialised practice between regulatory/policy advice and litigation in the TMT sector, and in EU/national Competition Law, Data Protection & Cybersecurity, emerging digital technologies (such as Artificial Intelligence, IoT and Robotics), Intellectual Property rights advocacy and compliance. Prior to founding the firm, Nikos held the post of General Counsel – Legal and Regulatory Affairs Director for a major telecoms operator and internet provider in Greece. He also held the position of Senior In-house Adviser to the EETT, responsible for Competition Law and Regulatory Policy/Compliance. He has filled senior consulting roles in various international projects for governments, national regulatory authorities, market players and the European Commission. Nikos has been a Visiting Lecturer on Electronic Communications Law, Data Protection & Cybersecurity, Competition Law and Intellectual Property at the AIT Center and the National Technical University of Athens. He is the author of numerous contributions in books and refereed journals in the fields of TMT, New Technologies and Competition Law.

Nikolinakos & Partners Law Firm
182, Mesogeion Avenue
15561, Athens
Greece

Tel: +30 213 002 0020
Email: nikolinakos@nllaw.gr
LinkedIn: www.linkedin.com/in/dnikolinakos



Dina Th. Kouvelou is a Partner, head of the Data Protection & Cybersecurity practice and co-head of the Competition Law, TMT and Digital Business practices of Nikolinakos & Partners Law Firm. Dina is recommended as a leading TMT, Data Protection and Competition Legal Counsel by *The Legal 500* (“an outstanding regulatory counsel” who “provides a hard-to-find combination of technical and practical legal advice”) and *Chambers and Partners* (“a true TMT expert”, “a competition law expert who is extremely business oriented, proactive, and an effective strategist”). During the last 20 years, Dina’s professional career has spanned TMT, Data Protection & Cybersecurity, Betting and Gaming, Competition Law and Corporate/Commercial Law, with experience in, among others, the following roles: General Counsel and Head of Legal & Regulatory Affairs in a leading alternative fixed telecoms operator and in a mobile operator in Greece; Senior Competition Law and Regulatory Policy Advisor in the Legal Department of the EETT; and Legal Consultant in Regulatory, Competition Law and Commercial Law projects with Greek and international law firms and consultancies.

Nikolinakos & Partners Law Firm
182, Mesogeion Avenue
15561, Athens
Greece

Tel: +30 213 002 0020
Email: kouvelou@nllaw.gr
LinkedIn: www.linkedin.com/in/dina-kouvelou-b26b5844



Alexis N. Spyropoulos is a Partner and Head of the Administrative Law & Public Procurement Practice of Nikolinakos & Partners Law Firm. From 2007 to 2015, he acted as Head of the Legal Department of the EETT, handling numerous complaints, actions and infringement proceedings. Alexis is experienced in representing undertakings and Government bodies in all kinds of proceedings (including Competition Law and Data Protection issues) before administrative courts and regulatory authorities. He has extensive (20 years) experience in the fields of TMT, Administrative Law, Data Protection and Competition Law.

Nikolinakos & Partners Law Firm
182, Mesogeion Avenue
15561, Athens
Greece

Tel: +30 213 002 0020
Email: spyropoulos@nllaw.gr
LinkedIn: www.linkedin.com/in/alexis-spyropoulos-359878125

Nikolinakos & Partners is an Athens-based law firm built upon a strong regulatory, transactional and litigation foundation. Our specialisation covers, *inter alia*, the following areas: TMT; Emerging Digital Technologies (including Artificial Intelligence, IoT and Robotics); Tech Disputes; Data Protection; Cybersecurity; Product Liability Litigation/Business Litigation; Competition Law; Intellectual Property; and Administrative Law. The firm is ranked #1 in Greece by the most prestigious international legal directories (for the 14th consecutive year) in TMT, Digital Business, Data Protection and Cybersecurity. The firm is also highly recommended in the areas of Litigation, Competition Law and Intellectual Property.

www.nllaw.gr



Hungary



Adam Liber



Tamás Bereczki

BLB Legal – Bagdi-Liber-Bereczki Attorneys-at-Law

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

Since 2018, the principal data protection law in Hungary is the General Data Protection Regulation (Regulation (EU) 2016/679; “GDPR”).¹

1.2 Is there any other general legislation that impacts data protection?

Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information (“Information Act”)² in Hungary serves as the primary legislation implementing the EU’s Law Enforcement Directive.³

1.3 Is there any sector-specific legislation that impacts data protection?

Act XLVII of 1997 on the Processing and Protection of Health and Related Personal Data (“Health Data Act”) lays down the detailed rules for the processing and the professional secrecy obligations of medical personnel.

Act XXI of 2008 on the Protection of Human Genetic Data and the Regulation of Human Genetic Studies, Research and Biobanks regulates the processing of human genetic data, including the transfer of such data to other countries.

Hungary has incorporated the EU Directive on privacy and electronic communications into its national law, primarily through Act CVIII of 2001 on Electronic Commerce and Information Society Services and Act C of 2003 on Electronic Communications.

In addition to the above, there are several laws that contain relevant data protection-related provisions, such as the Labour Code, Criminal Code,⁴ Civil Code,⁵ Act LIII of 2018 on the Protection of Privacy,⁶ Act XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities, etc.

1.4 What authority(ies) are responsible for data protection?

The Hungarian National Authority for Data Protection and Freedom of Information (“NAIH”) is Hungary’s independent data protection authority, responsible for enforcing data protection

laws and promoting the secure handling of personal data. It issues guidance, conducts audits and investigations, oversees breach notifications, and provides advisory support. The NAIH also has the power to impose sanctions and initiate legal action against violations.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **“Personal Data”**
Any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- **“Processing”**
Any operation or set of operations that is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- **“Controller”**
The natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
- **“Processor”**
A natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller.
- **“Data Subject”**
An identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological,

genetic, mental, economic, cultural or social identity of that natural person.

- **“Sensitive Personal Data”/“Special Categories of Personal Data”**
Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.
- **“Data Breach”**
A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
- **“Pseudonymous Data”**
The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
- **“Profiling”**
Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

3 Territorial and Material Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The GDPR applies to the processing of personal data of individuals in the EU by non-EU controllers or processors when offering goods or services or monitoring behaviour within the EU, and also applies where EU Member State law governs processing under public international law.

3.2 Do the data protection laws in your jurisdiction carve out certain processing activities from their material scope?

The GDPR does not apply to personal data processing that falls outside EU law, is conducted by Member States under Chapter 2, Title V of the TEU, is for purely personal or household use, or is carried out by competent authorities for criminal law enforcement or public security purposes.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Fairness**
Data subjects must be duly informed that their personal data will be processed, including comprehensive information regarding its collection, storage, and use, in order to allow data subjects to make informed decisions about

such processing and enable them to exercise their data protection rights.

- **Lawfulness**
Processing of personal data shall be lawful only if and to the extent that at least one of the lawful bases set out in Article 6 of the GDPR applies.
- **Transparency**
Any information addressed to the public or to the data subject shall be concise, easily accessible and easy to understand, and clear and plain language and, additionally, where appropriate, visualisation shall be used.
- **Purpose limitation**
Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- **Data minimisation**
Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- **Retention (storage limitation)**
Personal data shall be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.
- **Accuracy**
Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- **Integrity and confidentiality**
Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- **Accountability**
The controller shall be responsible for and be able to demonstrate compliance with the above principles.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to (copies of) data/information about processing**
Data subjects have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, if so, to access that data along with information about its purpose, categories, recipients, retention, source, rights regarding its processing, any automated decision-making, and to receive a copy of the data.
- **Right to rectification of errors**
The data subject has the right to request the prompt correction of any inaccurate personal data held by the controller. In line with the purposes of the processing, the data subject may also request that incomplete

personal data be completed, which may include the submission of a supplementary statement.

- **Right to deletion/right to be forgotten**

The data subject has the right to request the erasure of their personal data without undue delay, and the controller must comply when any of the following conditions apply: the data is no longer needed for its original purpose; the data subject withdraws consent and no other legal basis exists; the data subject objects to processing and there are no overriding legitimate grounds, or the objection concerns direct marketing; the data has been processed unlawfully; erasure is required to comply with a legal obligation under EU or national law; or the data was collected in relation to information society services offered to a child.

- **Right to object to processing**

The data subject has the right to object, at any time and on grounds relating to their particular situation, to the processing of their personal data where such processing is based on the performance of a task carried out in the public interest or in the exercise of official authority, or on the basis of legitimate interests pursued by the controller or a third party. This right also applies to any profiling based on these legal grounds.

- **Right to restrict processing**

Data subjects have the right to request restriction of processing of their personal data when its accuracy is contested, processing is unlawful but erasure is not desired, the data is no longer needed by the controller but required for legal claims, or an objection to processing is pending decision.

- **Right to data portability**

The data subject has the right to receive the personal data they have provided to a controller in a structured, commonly used, and machine-readable format. They also have the right to transmit that data to another controller without interference from the original controller, provided that the processing is based on the data subject's consent or on a contract, and the processing is carried out by automated means.

- **Right to withdraw consent**

The data subject has the right to withdraw their consent at any time. Such withdrawal does not affect the lawfulness of any processing carried out based on consent prior to its withdrawal. Before consent is given, the data subject must be informed of this right. Withdrawing consent must be as straightforward as giving it.

- **Right to object to marketing**

Where personal data is processed for direct marketing purposes, the data subject has the right to object at any time to such processing. This includes any profiling activities that are related to direct marketing.

- **Right protecting against solely automated decision-making and profiling**

Data subjects have the right not to be subject to decisions based solely on automated processing, including profiling, if those decisions have legal or similarly significant effects.

- **Right to complain to the relevant data protection authority(ies)**

Data subjects have the right to lodge a complaint with the NAIH if they believe that the processing of their personal data violates applicable data protection laws.

- **Right to compensation**

In the event of violation of the right to the protection of personal data, the data subject may seek compensation for pecuniary or non-pecuniary damages caused by the unlawful processing of personal data under the Hungarian Civil Code.

5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

Yes, under Hungarian law, there is a mechanism for collective redress, specifically through representative actions, regarding data protection rights, which can be initiated by qualified not-for-profit organisations.

6 Children's Personal Data

6.1 What additional obligations apply to the processing of children's personal data?

When offering online services to children, processing their data is lawful only with parental consent if they are under 16, and all information must be communicated in clear, child-friendly language.

7 Registration Formalities and Prior Approval

7.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

The GDPR requires controllers and most processors to maintain records of their processing activities without registering with or notifying the NAIH.

7.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

This is not applicable.

7.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

This is not applicable.

7.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

This is not applicable.

7.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

This is not applicable.

7.6 What are the sanctions for failure to register/notify where required?

This is not applicable.

7.7 What is the fee per registration/notification (if applicable)?

This is not applicable.

7.8 How frequently must registrations/notifications be renewed (if applicable)?

This is not applicable.

7.9 Is any prior approval required from the data protection regulator?

This is not applicable.

7.10 Can the registration/notification be completed online?

This is not applicable.

7.11 Is there a publicly available list of completed registrations/notifications?

This is not applicable.

7.12 How long does a typical registration/notification process take?

This is not applicable.

8 Appointment of a Data Protection Officer

8.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

A Data Protection Officer (“DPO”) is required for public bodies, or when core activities involve large-scale monitoring or processing of special categories of data; voluntary DPOs must also meet all GDPR obligations.

8.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

Failing to appoint a DPO in cases where the appointment is mandatory may result in an administrative fine of up to EUR

10 million, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

8.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

Hungarian law does not shield DPOs from disciplinary actions, although the Information Act requires them to maintain confidentiality, with violations potentially leading to consequences.

8.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

A group of undertakings may appoint a single DPO, provided the DPO is easily accessible from each establishment.

8.5 Please describe any specific qualifications for the Data Protection Officer required by law.

Although no specific qualification is required by law for the DPO, he or she shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices.

8.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

The DPO advises and informs on data protection obligations, monitors compliance and internal policies, oversees Data Protection Impact Assessments (“DPIAs”), cooperates with supervisory authorities, acts as their contact point, and helps develop data protection and security policies.

8.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

Yes, the registration may be carried out through a dedicated electronic interface, in addition to the other available means of contact. The data of the DPO is publicly disclosed by the NAIH.⁷

8.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

Yes, the contact details of the DPO must be publicly disclosed. The most common way is disclosure of the contact details in a publicly facing privacy notice. In addition, the controller or processor must notify the NAIH of the DPO’s name, postal address and email, which are disclosed to the public by the NAIH.

9 Appointment of Processors

9.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes. Processing by a processor must be governed by a contract or other legal act under EU or Member State law.

This agreement must be binding on the processor and define the subject matter, duration, nature, and purpose of the processing, the types of personal data, categories of data subjects, and the controller's obligations and rights.

9.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

A data processing agreement must be in writing, including in electronic form, detailing the processing scope, duration, purpose, data types, data subjects, and the controller's rights. It must require the processor to follow documented instructions, ensure confidentiality, apply GDPR-compliant security, manage sub-processors properly, assist with data subject rights and compliance, return or delete data after the end of service, and provide audit support.

10 Marketing

10.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

Under Act XLVIII of 2008 on Business Advertising Activity, direct marketing communications (e.g., via email or similar channels) to natural persons require the recipient's prior, explicit, and unambiguous consent. These may be sent without prior consent if recipients are clearly informed of their right to opt out at any time, free of charge and without restriction.

Additionally, the E-Commerce Act stipulates that using services for purposes like targeted advertising, service improvement, or market research is only permitted if the purpose of data processing is defined in advance and the user has consented.

10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

The explicit opt-in consent of the targeted individual and this consent requirement is independent from the B2B or B2C standing of the recipient.

10.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

Under Act C of 2003 on Electronic Communications, automated calls for direct marketing require the subscriber's prior consent. In contrast, live marketing calls are allowed without prior consent unless the individual has opted out. For postal marketing, addressed advertising materials (i.e., postal items – not specifically named in the Postal Services Act – sent simultaneously to at least 500 recipients, with identical content except for data that do not alter the nature of the message, such as the recipient's name and address) may be sent without prior consent, provided recipients can opt out at any time, free of charge and without restriction.

10.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Yes, the restrictions mentioned in above points apply to marketing directed to Hungary.

10.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

The NAIH handles data protection in marketing, while the National Media and Infocommunications Authority ("NMHH") oversees advertising related to information society services and advertising carried out via electronic communications – with the exception of voice-based telephone calls. The Hungarian Competition Authority ("HCA") and the Hungarian Consumer Protection Authorities are in charge regarding the prosecution of unfair commercial practices against consumers.

10.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Yes, it is lawful, but only if the data subject consented to the transfer of their personal data to a third party and if there is a legal basis for the processing of personal data for marketing purposes.

10.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Failing to send marketing communications in accordance with the applicable law may result in an administrative fine up to EUR 20 million, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher. Regarding unfair commercial practices violations, the HCA may impose a monetary fine up to 15% of the total worldwide annual turnover of the preceding financial year of the relevant undertaking.

11 Cookies

11.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

In Hungary, the use of cookies is governed by the ePrivacy Directive, implemented through Act CVIII of 2001 ("E-Commerce Act") and complemented by the GDPR where personal data is involved. Additionally, Act C of 2003 on Electronic Communications requires that data may only be stored on or accessed from a user's device with clear, comprehensive information and the user's consent, including the purpose of processing.

Cookies must be categorised by purpose. Non-essential cookies – such as those used for analytics, marketing, or personalisation – require explicit prior consent. Essential cookies, necessary for communication or services explicitly requested by the user, are exempt from this requirement. However, transparency is always mandatory: users must be clearly informed about the types of cookies used, their functions, and the extent of data processing involved.

11.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

The practice of the NAIH distinguishes between cookies that (i) are technically essential for the provision of the information society service, and (ii) other cookies that are technically not essential, i.e., require the consent of the user (e.g., analytical, marketing cookies).

11.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

In case no. NAIH-3195-11/2022, the Hungarian data protection authority imposed a fine of HUF 10 million on the data controller due to a lack of (i) proper information provision to users in connection with cookies, and (ii) transparent and clear consent management.

11.4 What are the maximum penalties for breaches of applicable cookie restrictions?

Failing to comply with the applicable cookie restrictions may result in an administrative fine up to EUR 20 million, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

12 Restrictions on International Data Transfers

12.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Personal data may only be transferred outside the EEA if one of the following applies: (i) the destination country has an EU adequacy decision; (ii) appropriate safeguards (e.g., standard contractual clauses (“SCCs”)) are in place; or (iii) a derogation under Article 49 GDPR applies – used only as a last resort, especially in international relations. Data controllers must document these decisions to meet GDPR accountability requirements and may need to consult or obtain authorisation from the NAIH in certain cases.

12.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

When transferring personal data to countries without an EU adequacy decision, companies must implement GDPR-compliant safeguards, typically using SCCs. Alternatively, transfers may rely on custom contracts with prior NAIH approval, provided they include adequate protections. For intra-group transfers, businesses can adopt Binding Corporate Rules, which must be approved by the NAIH and be legally binding, clearly outlining the group structure, transfer purposes, data subject rights, compliance measures, and complaint procedures.

12.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

Personal data transfers within the EEA or to countries with an EU adequacy decision generally do not require notification. However, *ad hoc* contractual clauses need prior NAIH authorisation, and transfers based on “compelling legitimate interests” under Article 49(1)(2) GDPR must be notified to the NAIH.

For genetic data, the Genetic Data Act requires that any international transfer for research or testing be reported to Hungary’s Chief Public Health Officer, including details of the safeguards used by both sender and recipient.

12.4 Do transfers of personal data to other jurisdictions require a transfer impact assessment? If conducting a transfer impact assessment is only mandatory in some circumstances, please identify those circumstances.

Before transferring data to a non-EU country without an adequacy decision, controllers or processors must assess whether its legal framework ensures EU-equivalent protection through a transfer impact assessment.

12.5 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?

The European Data Protection Board’s Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data⁸ were issued in light of the *Schrems II* decision.

12.6 What guidance (if any) has/have the data protection authority(ies) issued in relation to the use of standard contractual/model clauses as a mechanism for international data transfers?

On 4 June 2021, the European Commission adopted updated SCCs⁹ under the GDPR for international data transfers from EU/EEA-based controllers or processors to processors located outside the EU/EEA that are not subject to the GDPR. These modernised SCCs supersede the three earlier sets of clauses adopted under the former Data Protection Directive 95/46/EC.

13 Whistle-blower Hotlines

13.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

Under Hungary’s Act XXV of 2023 (“Complaints Act”), implementing the Whistleblower Directive EU/2019/1937, individuals can report unlawful or suspected misconduct through an internal whistleblowing system. Eligible reporters include: current, former, and prospective employees; contractors and their representatives; interns, volunteers, and applicants in

ongoing recruitment; as well as individuals whose relationship with the employer has ended. Duplicate reports with identical content may be ignored, and reports submitted more than six months after becoming aware of the issue – or more than one year after the event – may be disregarded.

13.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Under the Hungarian Whistleblowing Act, individuals are generally permitted to report unlawful acts and other abuses without revealing their identity. However, anonymous reports where the reporting person cannot be identified may be disregarded.

14 CCTV

14.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

No. The use of CCTV does not require any separate registration/notification or prior approval from the NAIH. However, conducting DPIA may be mandatory if CCTV is used, for example, for personal and property protection purposes, detection, prevention and suppression of crimes.

14.2 Are there limits on the purposes for which CCTV data may be used?

The use of CCTV systems must comply with the GDPR and be based on lawful, specific, and legitimate purposes. CCTV may be used for asset protection, but is prohibited in areas where it could infringe on human dignity, such as changing rooms, restrooms, hospital rooms, and residential areas of social institutions. The NAIH recently clarified that household surveillance qualifies as an exemption from the GDPR only if monitoring is strictly limited to the private property or, in exceptional cases, minimally extends to its immediate surroundings when necessary for security. Even then, surveillance must be configured to avoid capturing footage beyond the property unless essential, and appropriate safeguards must be in place to protect others' privacy.

15 Employee Monitoring

15.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Employers in Hungary may monitor employees for work-related purposes without prior consent, provided the methods respect human dignity, are proportionate and limited, exclude private life and correspondence, and comply with data protection laws.

15.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Employers are obligated to inform employees in advance about any restrictions on their privacy rights, including the nature,

conditions, and anticipated duration of such limitations. Additionally, employers must provide written notice detailing any data processing activities and the implementation of technical monitoring tools.

15.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

Employers are required to consult with the works council before implementing any measures or internal policies that significantly affect a large number of employees. This consultation obligation extends to matters involving the processing and protection of employee personal data, as well as the deployment of technical tools used for employee monitoring.

15.4 Are employers entitled to process information on an employee's attendance in office (e.g., to monitor compliance with any internal return-to-office policies)?

The Hungarian Labour Code allows employers to monitor employees in connection with their conduct related to the employment relationship, which can also entail the monitoring of employee attendance in the office.

16 Data Security and Data Breach

16.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Yes, there is. Controllers and processors must ensure data security through appropriate safeguards – like encryption and pseudonymisation – protecting personal data from unauthorised access, loss, or misuse, etc.

16.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

In Hungary, data controllers must report personal data breaches to the NAIH without undue delay, no later than 72 hours after becoming aware of the breach, and with the details described in the GDPR, unless it is unlikely to pose a risk to individuals' rights and freedoms.

16.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

If a data breach poses a high risk to individuals, the controller must promptly notify them without undue delay in clear language, detailing the breach, contact point, likely consequences, and mitigation steps. Notification is not required if effective safeguards were already in place.

16.4 What are the maximum penalties for personal data security breaches?

An administrative fine of up to EUR 10 million, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year – whichever is higher – may be imposed.

17 Enforcement and Sanctions

17.1 Describe the enforcement powers of the data protection authority(ies).

- (a) **Investigative powers:** The NAIH is responsible for enforcing data protection laws, issuing guidelines, and ensuring organisations uphold strong data security standards. It conducts audits and investigations to assess compliance. If no breach is found, the case is closed. If unlawful data processing is identified, the NAIH may order corrective action. Failure to comply or severe breaches can lead to an administrative procedure, confidentiality oversight procedure, as well as the NAIH may also initiate court proceedings, or prepare a report.
- (b) **Corrective powers:** The NAIH has extensive corrective powers to ensure compliance. These include issuing warnings or reprimands, ordering data controllers to fulfil data subject rights or notify individuals of data breaches, and imposing temporary or permanent bans on processing. They can also withdraw certifications, suspend international data transfers, and impose significant administrative fines.
- (c) **Authorisation and advisory powers:** The NAIH is granted a broad set of powers to ensure compliance and promote accountability among data controllers and processor. These powers include both advisory and authorisation roles.
- (d) **Imposition of administrative fines for infringements of specified legal provisions:** The NAIH may launch an administrative procedure – either *ex officio* or via complaints – as its main enforcement tool, independent of prior investigations. It can impose fines or corrective actions, guided by the European Data Protection Board (“EDPB”) Guidelines 04/2022. Under the Information Act, all case-specific factors must be considered to determine whether a fine is warranted and to set its amount.
- (e) **Non-compliance with a data protection authority:** Non-compliance with the NAIH may result in administrative fines amounting to EUR 20 million or up to 4% of the business’s worldwide annual turnover of the preceding financial year, whichever is higher.

17.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The NAIH has the power to enforce either a temporary or permanent restriction, including a complete ban, on processing activities, requiring no court order.

17.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

The NAIH, Hungary’s independent data protection authority, exercises structured investigative, corrective, authorisation,

advisory, and enforcement powers, including the imposition of administrative fines. In a 2024 case, the NAIH fined Aldi HUF 80 million for non-transparent age verification practices in alcohol sales, ordering corrective measures to standardise procedures.

The NAIH also uses its advisory powers proactively. Ahead of election periods, it regularly issues guidance to political parties on data protection compliance. Its most recent guidance, published in spring 2024, focused on the lawful processing of personal data in political marketing.

17.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

The NAIH exercises its tasks and powers with respect to legal entities under the jurisdiction of Hungary. The NAIH may order the removal or blocking of access to personal data published online as an interim measure if it can stop unlawful processing and prevent serious, irreparable harm if the data relates to a child, special categories of personal data (e.g., health, religion, sexual orientation), or criminal personal data. Non-compliance by hosting or intermediary providers may result in fines between HUF 100,000 and HUF 20 million. If removal is ineffective and serious harm remains likely, the NAIH may also order temporary blocking. Such orders are published and enforced with the involvement of the NMHH. Measures cease once proceedings conclude or the grounds for intervention no longer exist.

18 E-discovery/Disclosure to Foreign Law Enforcement Agencies

18.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Businesses typically evaluate such requests to ensure compliance with data protection laws, international treaties, including verifying the legal basis for personal data transfers and the adequacy of technical and organisational measures in place.

18.2 What guidance has/have the data protection authority(ies) issued on disclosure of personal data to foreign law enforcement or governmental bodies?

The NAIH has not yet issued any guidance on disclosure of personal data to foreign law enforcement or governmental bodies.

19 Artificial Intelligence

19.1 Are there any limitations on automated decision-making involving the processing of personal data using artificial intelligence?

Individuals have the right not to be subject to decisions based solely on automated processing, including profiling, that significantly affect them, unless it is based on explicit consent, necessary for a contract, or authorised by law with appropriate safeguards.

19.2 What guidance (if any) has/have the data protection authority(ies) issued in relation to the processing of personal data in connection with artificial intelligence?

The EDPB has adopted an opinion on the use of personal data in the development and deployment of artificial intelligence (“AI”) models.¹⁰ This opinion addresses: (i) the conditions under which AI models may be considered anonymous; (ii) the applicability of legitimate interest as a legal basis for processing personal data in AI contexts; and (iii) the implications of using unlawfully processed personal data in AI model development.

The NAIH has not issued any guidance regarding AI; however, in case no. NAIH-85-3/2022 it dealt in detail with data protection issues in the use of AI.

20 Trends and Developments

20.1 In your opinion, what enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.

Hungarian data protection enforcement is increasingly focused on emerging technologies like AI, alongside traditional areas such as direct marketing, workplace privacy, CCTV surveillance, cookie management, data subject rights, and covert audio recordings. The HCA has also recognised data protection as a component of consumer welfare, intervening where privacy violations constitute unfair commercial practices.

Relevant case law from the previous 12 months includes, among others, the following decisions:

- (i) A bank fined approx. EUR 145,000 for inadequate CCTV signage, emphasising that pictograms alone are insufficient and detailed notices must be placed at entrances.
- (ii) A ruling on private property surveillance, clarifying that household data processing is exempt from the GDPR only if monitoring is confined to private property or minimally extends to its immediate vicinity.
- (iii) The NAIH found that an organisation failed to properly handle data subjects’ requests to unsubscribe from newsletters and withdraw consent for marketing communications. Despite users opting out, the organisation continued to send emails, violating GDPR principles of lawfulness, fairness, and transparency.
- (iv) Aldi Hungary was fined approx. EUR 197,000 for unlawful data processing during alcohol sales, breaching data minimisation and purpose limitation rules.

In addition, several Hungarian court decisions clarify that the consequences of unauthorised data processing under the Information Act differ from those under the Civil Code, and claims for grievance awards for data processing violations must primarily rely on the Information Act’s framework.

20.2 In your opinion, what “hot topics” are currently a focus for the data protection regulator?

AI: The Hungarian government has adopted Resolution No 1301/2024 (IX. 30) on the implementation of the European Parliament and Council Regulation (2024/1689/EU) on AI in Hungary.

Cybersecurity: The 2024 Cybersecurity Act, effective from 1 January 2025, consolidates Hungary’s cybersecurity legal framework by repealing the 2023 Cybersecurity Act and other fragmented regulations. As part of the NIS2 implementation efforts, the Hungarian government also released Government Decree 418/2024 (XII. 23) on the Implementation of the 2024 Cybersecurity Act.

Looking ahead, it is expected that the regulator will continue to align with the dynamic evolution of regulatory frameworks in these areas, placing particular emphasis on the consistent and effective implementation of the relevant legal provisions in line with technical and data protection-related developments.

Endnotes

- 1 <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- 2 <https://njt.hu/jogszabaly/en/2011-112-00-00>
- 3 <https://eur-lex.europa.eu/eli/dir/2016/680/oj/eng>
- 4 <https://njt.hu/jogszabaly/en/2012-100-00-00>
- 5 <https://njt.hu/jogszabaly/en/2013-5-00-00>
- 6 <https://njt.hu/jogszabaly/en/2018-53-00-00>
- 7 <https://dpo-online.naih.hu>
- 8 https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en
- 9 https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj
- 10 https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_en



Adam Liber, a seasoned partner at Provaris, specialises in data protection, IT, intellectual property, and competition law. With over 15 years in the field, he co-leads legal teams and is a certified intellectual property expert. He holds LL.M. degrees in Global and US Business Law and Competition Law, along with various international data protection certifications. Adam advises multinational corporations on EU data protection laws, oversees complex outsourcing, and manages international data transfers. He represents clients across multiple sectors in investigations, audits, and disputes involving digital technology and compliance. Additionally, Adam is an external expert for the European Data Protection Board's Support Pool and serves on the Legal Advisory Committee of the ADR Forum at the Council of Hungarian Internet Service Providers.

BLB Legal – Bagdi-Liber-Bereczki Attorneys-at-Law
Bank Center H-1054, Szabadság tér 7
Budapest
Hungary

Tel: +36 20 524 4959
Email: adam.liber@blblegal.hu
LinkedIn: www.linkedin.com/in/adam-liber



Tamás Bereczki, a partner at Provaris, is an expert in data protection, cyberlaw, information security, IT, and technology. He has practical experience in information security management, risk assessments, ISO 27001 management systems, privacy frameworks, incident and cybersecurity management, as well as third-party and cloud service risk management in various sectors like finance, air transportation, pharmaceuticals, and e-commerce. Tamás possesses degrees in Law and Computer Science, along with notable certifications such as CISM and CRISC from ISACA, and CIPP/E from the IAPP. He co-chairs the *IAPP KnowledgeNet* Hungary Chapter and is a recognised expert at the European Data Protection Board's Support Pool of Experts.

BLB Legal – Bagdi-Liber-Bereczki Attorneys-at-Law
Bank Center H-1054, Szabadság tér 7
Budapest
Hungary

Tel: +36 30 220 2428
Email: bereczki.tamas@provaris.hu
LinkedIn: www.linkedin.com/in/tamas-bereczki-13984739

The firm was established by seasoned lawyers who have received broad recognition from several leading legal directories, including *Chambers and Partners* and *The Legal 500*, at both individual and departmental levels. Our professional reputation in these areas has been built and sustained through work on a wide range of regulatory and dispute-related matters, including complex cross-border data protection and international data transfer compliance issues. We possess deep experience in various technology and digitalisation solutions, data protection management software, and cross-border compliance tools. Our understanding of the nuances of operating in highly competitive, cutting-edge multinational environments enables us to guide clients effectively through the complexities of legal challenges. BLB Legal offers market-leading advisory capabilities in technology and cybersecurity. We regularly provide business consultancy services with a particular focus on compliance with various cybersecurity

frameworks, including DORA, NIS2 and other related regulation. We assist numerous multinational companies in structuring both their internal and external data transfers within and outside the European Union, managing vendor relationships, and mitigating regulatory risks.

www.blblegal.hu



India

AZB & Partners



Rachit Bahl



Rohan Bagai



Sumit Ghoshal



Archana Iyer

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The Digital Personal Data Protection Act, 2023 (“**DPDP Act**”), enacted on August 11, 2023, is India’s principal data protection legislation. As of May 2025, while the DPDP Act has been enacted, its substantive provisions are yet to be notified and enforced. On January 3, 2025, the competent ministry under the Government of India, the Ministry of Electronics and Information Technology (“**MeitY**”), released the Draft Digital Personal Data Protection Rules, 2025 (“**Draft Rules**”), for public consultation. The DPDP Act and the Draft Rules are expected to be enforced in a phased manner, with sufficient sunrise period provided to organisations to transition to the new data protection regime.

Until the DPDP Act is enforced, the current data protection regime is contained under the provisions of the Information Technology Act, 2000 (“**IT Act**”). Section 43A of the IT Act holds a body corporate liable for negligence in implementing reasonable security practices while handling sensitive personal data; and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (“**SPDI Rules**”), notified under the IT Act, set out procedures for lawful collection, use, transfer and disclosure of sensitive personal data.

Once the DPDP Act is enforced, it will repeal the existing regime under the IT Act and the SPDI Rules entirely. Given the limited enforcement of the SPDI Rules and the reported expectation of the Government for organisations to move towards compliance with the DPDP Act, we have discussed the relevant provisions of the DPDP Act in this chapter.

1.2 Is there any other general legislation that impacts data protection?

Yes. Some of the other general legislation that may directly or indirectly impact data protection include the following: (a) the IT Act prescribes penalties and consequences for unauthorised access to data and disclosure of data in breach of a lawful contract; (b) the Information Technology (Indian Computer Emergency Response Team (“**CERT-In**”) and Manner of Performing Functions and Duties) Rules, 2013, notified under the IT Act, prescribe mandatory reporting of cyber security incidents including data breaches and data leaks; (c) the CERT-In has issued binding directions under the IT Act, requiring entities to retain information and communication

technology system logs, report cyber incidents and cybersecurity incidents within strict timelines, etc.; (d) the Consumer Protection Act, 2019, proscribes unfair trade practices, which includes disclosing to another person any personal information given in confidence by the consumer unless such disclosure is in accordance with applicable law; and (e) the *Bhartiya Nyaya Sanhita*, 2023 (which has repealed and replaced the Indian Penal Code, 1860), contains provisions that impose criminal liability for acts such as identity theft, impersonation, cheating, theft of movable property and criminal breach of trust, which may involve misuse of personal information.

1.3 Is there any sector-specific legislation that impacts data protection?

Yes. While the DPDP Act and the IT Act (read with the SPDI Rules) constitute the primary legal framework for data protection in India, several sector-specific legislation and regulatory guidelines such as those prescribed by the Securities and Exchange Board of India, the Reserve Bank of India (“**RBI**”), the Insurance Regulatory and Development Authority of India (“**IRDAI**”) and the Telecom Regulatory Authority of India (“**TRAI**”) impose certain obligations that impact the processing of customer data, which may include personal data. For instance, the RBI’s Guidelines on Cyber Security Framework in Banks, Master Directions on Digital Payment Security Controls and Outsourcing of IT Services, Master Direction – Know Your Customer (KYC) Direction, 2016, etc., require regulated entities to implement adequate data protection to protect the integrity and security of data, and customer confidentiality.

Similarly, the IRDAI mandates insurers to establish robust governance mechanisms for protecting policyholder information. Its guidelines require insurers to implement information security policies, ensure confidentiality of customer data and adopt risk-based controls, particularly when outsourcing functions to third-party service providers.

1.4 What authority(ies) are responsible for data protection?

The DPDP Act contemplates the establishment of the Data Protection Board of India (“**DPB**”), which will serve as the enforcement and adjudicatory body under the DPDP Act and will be responsible for functions including inquiring into personal data breaches, directing remedial action and imposing penalties for non-compliance with the DPDP Act.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **“Personal Data”**
The DPDP Act defines “Personal Data” as “any data about an individual, who is identifiable by or in relation to such data”.
- **“Processing”**
The DPDP Act defines “Processing” in relation to personal data as a wholly or partly automated operation or set of operations performed on digital personal data and includes operations such as collection, recording, organisation, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise, making available, restriction, erasure or destruction.
- **“Controller”**
The DPDP Act uses the term Data Fiduciary (akin to a controller), defined as “any person who, alone or in conjunction with other persons, determines the purpose and means of the processing of personal data”.
- **“Processor”**
The DPDP Act defines a Data Processor as “any person who processes personal data on behalf of a Data Fiduciary”.
- **“Data Subject”**
The DPDP Act defines and uses the term “Data Principal” (akin to data subjects) as the individual to whom the personal data relates and where such individual is: (i) a child, including parents or lawful guardians of such a child; or (ii) a person with a disability, including her lawful guardian, acting on her behalf.
- **“Sensitive Personal Data”/“Special Categories of Personal Data”**
The DPDP Act does not sub-categorise personal data into “Sensitive Personal Data” or “Special Categories of Personal Data”.
- **“Data Breach”**
The DPDP Act defines “personal data breach” to mean any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data.
- **“Automated”**
The term “automated” has been defined to mean any digital process capable of operating automatically in response to instructions given or otherwise for the purpose of processing data.

3 Territorial and Material Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

Yes, the DPDP Act has extraterritorial applicability and extends to entities established outside India where the processing is carried out outside India in connection with offering goods or services to data principals located within India.

3.2 Do the data protection laws in your jurisdiction carve out certain processing activities from their material scope?

Yes. The DPDP Act applies only to: (a) digital personal data (i.e., personal data in digitised form); and (b) personal data collected in non-digital form that is subsequently digitised, and does not apply to: (i) personal data processed by an individual for any personal or domestic purpose; (ii) personal data that is made or is caused to be made publicly available by the data principal, or by a person under a legal obligation; (iii) processing by notified Central or State agencies in the interests of security of State, friendly relations with foreign States, maintenance of public order, etc.; and (iv) processing necessary for research, archiving or statistical purposes, if such personal data is not used for decision making and is carried out in accordance with prescribed standards.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
The principle of transparency permeates the provisions of the DPDP Act. For instance, data fiduciaries are required to provide clear, comprehensive and easily accessible notices to data principals to obtain specific and informed consent from data principals, including setting out prescribed details such as categories of personal data to be processed and the purpose of the processing, the manner of exercise of rights available to the data principal, and the mechanism to make a complaint to the DPB. Further, the data principals are provided with rights to access information, including summary of processing activities undertaken by a data fiduciary, identities of all data fiduciaries and data processors with whom their personal data has been shared, etc.
- **Lawful basis for processing**
The DPDP Act mandates that personal data should be processed only in a lawful manner and for lawful purposes, and in accordance with the provisions contained therein. It contemplates two distinct legal bases for such processing: (i) consent; and (ii) certain legitimate uses. As per Section 6 of the DPDP Act, processing of personal data may be undertaken with the free, specific, informed, unconditional and unambiguous consent of the data principal, obtained through clear affirmative action. Further, Section 7 of the DPDP Act also sets out nine specific “legitimate uses” for processing personal data without consent, such as for the purpose of employment, where processing is necessary for the performance of a legal function, compliance with a judgment or order, etc.
- **Purpose limitation**
The principle of purpose limitation can be inferred from various provisions of the DPDP Act. Section 6(1) of the DPDP Act provides that the consent provided by the data principal will signify an agreement to the processing of her personal data for the specified purpose set out in the notice provided to them. The principle also applies in the context of legitimate uses specified under Section 7 of the DPDP Act, which permits processing only for certain identified use-cases, such as for the purpose of employment, performance of legal functions, etc.

■ **Data minimisation**

The principle of data minimisation can be inferred from various provisions of the DPDP Act. Section 6 of the DPDP Act states that consent provided by the data principal will be limited to such personal data as is necessary for the specified purpose for which personal data is collected as set out in the privacy notice provided to them.

■ **Proportionality**

This principle is reflected in multiple provisions of the DPDP Act that collectively require that the extent, manner and duration of processing of personal data (either with explicit consent or for legitimate use cases) must bear a reasonable nexus to the permitted purpose for which the personal data is being processed.

■ **Retention**

The DPDP Act provides that the personal data of a data principal may be retained only until (a) the data principal withdraws consent, or (b) as soon as it is reasonable to assume that the specified purpose is no longer being served, unless retention is required to ensure compliance with applicable law.

■ **Accuracy**

Section 8(3) of the DPDP Act requires that every data fiduciary ensure that personal data processed by it is complete, accurate and consistent, particularly where such data is used for decision making or is disclosed to another data fiduciary.

■ **Accountability**

While the term “accountability” is not expressly used, the DPDP Act effectively embeds this principle by providing that the data fiduciary will be responsible for ensuring compliance with the provisions of the DPDP Act, including with respect to any processing carried out on its behalf by a data processor, including by way of implementation of appropriate technical and organisational measures, adoption of reasonable security safeguards to prevent personal data breach, facilitation of exercise of data principal rights, obligation to notify personal data breaches to both the DPB and the affected data principals, etc.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

■ **Right of access to (copies of) data/information about processing**

The DPDP Act confers upon the data principal, the right to access information about her personal data, which includes obtaining from the data fiduciary, a summary of the personal data being processed in relation to her, details regarding the purpose of processing and the categories of data fiduciaries or data processors with whom such data has been shared.

■ **Right to rectification of errors**

The DPDP Act provides the data principal with the right to request the data fiduciary for the correction, completion or updating of her personal data for which she has previously given her consent, or for certain specified purposes for which the data principal has voluntarily provided such personal data.

■ **Right to deletion/right to be forgotten**

The DPDP Act provides data principals with the right to request erasure of their personal data, where such personal data was provided either based on consent or

where the personal data has been voluntarily provided by the data principal for a specified purpose. In such cases, a data fiduciary is obligated to erase the data unless its retention is necessary to fulfil the original purpose or comply with legal obligations.

■ **Right to object to processing**

The DPDP Act does not recognise a standalone right to object to the processing of personal data. However, where processing is based on consent, the right to withdraw consent may be exercised specifically in relation to particular instances of processing.

■ **Right to restrict processing**

The DPDP Act does not confer a general right to restrict processing of personal data. However, where processing is based on consent or voluntarily provided personal data for a specified purpose, data principals may exercise their right to update or correct personal data, withdrawal of consent and/or right to erasure.

■ **Right to data portability**

The DPDP Act does not provide an express right to data portability.

■ **Right to withdraw consent**

The DPDP Act confers on the data principal the right to withdraw her consent at any time with comparable ease with which such consent was given. Such withdrawal of consent does not affect the lawfulness of processing undertaken prior to such withdrawal.

■ **Right to object to marketing**

The DPDP Act does not confer an express right to object to direct marketing. However, since consent is likely the primary basis for processing personal data for marketing purposes, the data principal may withdraw consent for such purpose at any time.

■ **Right protecting against solely automated decision-making and profiling**

The DPDP Act does not contain any express provisions restricting or regulating automated decision-making or profiling. However, please see our response to question 6.1 on prohibitions relating to children’s data and question 19.1 for additional obligations on Significant Data Fiduciaries (“SDFs”) for use of automated software.

■ **Right to complain to the relevant data protection authority(ies)**

The DPDP Act provides data principals with the right to complain to the DPB in respect of any breach of obligations by a data fiduciary or a consent manager. This right is subject to the prior exhaustion of the data fiduciary’s grievance redressal mechanism.

■ **Other key rights:**

■ **Right to grievance redressal:** Section 13 of the DPDP Act provides data principals with the right to have a readily available means of grievance redressal provided by a data fiduciary or consent manager regarding the performance of its obligations contained thereunder.

■ **Right to nominate:** Section 14 of the DPDP Act confers on data principals the right to nominate one or more individuals to exercise their rights under the DPDP Act in the event of their death or incapacity.

5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

No, the DPDP Act does not provide any such right to data principals.

6 Children’s Personal Data

6.1 What additional obligations apply to the processing of children’s personal data?

Under the DPDP Act, data fiduciaries must obtain verifiable consent from a parent or guardian before processing a child’s personal data, with a child defined as an individual under 18 years of age. The Draft Rules require technical safeguards to ensure consent and due diligence to verify the adult’s identity, using existing data or voluntarily provided details including authorised credentials like virtual tokens. The DPDP Act also prohibits tracking, targeted advertising and harmful processing of children’s data. Pursuant to enabling provisions under the DPDP Act, the Central Government proposes to exempt certain data fiduciaries such as healthcare, education and childcare providers from consent and monitoring restrictions, provided processing is limited to necessary functions for child welfare.

7 Registration Formalities and Prior Approval

7.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

No, under the DPDP Act, there is no general obligation for data fiduciaries to register with or notify the DPB merely by virtue of engaging in personal data processing. That said, the Draft Rules envisage a specific registration requirement for entities intending to function as consent managers, which is an entity that enables a data principal to give, manage, review and withdraw consent through an accessible, transparent and interoperable platform. Rule 4 of the Draft Rules propose that a consent manager is required to obtain registration from the DPB as per the prescribed eligibility conditions, including the requirement for it to be a company incorporated in India, and other obligations that must be satisfied or fulfilled prior to and during the term of such registration.

7.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

Please refer to our response to question 7.1 above.

7.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

Please refer to our response to question 7.1 above.

7.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

Please refer to our response to question 7.1 above.

7.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

Please refer to our response to question 7.1 above.

7.6 What are the sanctions for failure to register/notify where required?

Please refer to our response to question 7.1 above. Failure by a consent manager to obtain registration may attract penalties of up to INR 50 crores.

7.7 What is the fee per registration/notification (if applicable)?

Please refer to our response to question 7.1 above. Any fees for registration as a consent manager are currently not provided under the Draft Rules; however, they may be stipulated by the DPB.

7.8 How frequently must registrations/notifications be renewed (if applicable)?

Please refer to our response to question 7.1 above. The Draft Rules currently do not contemplate renewal of registration of a consent manager but provide for suspension or cancellation of registration upon any contravention by such entities of any of their obligations.

7.9 Is any prior approval required from the data protection regulator?

Please refer to our response to question 7.1 above. No such prior approval is required for a consent manager.

7.10 Can the registration/notification be completed online?

Please refer to our response to question 7.1 above. The DPB is envisaged to be a completely digital office and therefore, the registration process in respect of a consent manager is likely to be online.

7.11 Is there a publicly available list of completed registrations/notifications?

Please refer to our response to question 7.1 above. The Draft Rules provide for publication of particulars of registered consent managers on the DPB’s website.

7.12 How long does a typical registration/notification process take?

Please refer to our response to question 7.1 above. There are no timelines stipulated as of now under the Draft Rules for completion of the process of registration as a consent manager.

8 Appointment of a Data Protection Officer

8.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

All the data fiduciaries are required to publish, in the prescribed form, the business contact details of either (a) the Data Protection Officer (“DPO”) (if appointed), or (b) another designated person capable of addressing questions raised by the data principal regarding the processing of their personal data. The requirement to appoint a DPO arises only where a data fiduciary is designated as an SDF by the Central Government under Section 10(1) of the DPDP Act.

8.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

Failure to appoint a DPO may lead to monetary penalties of up to INR 150 crores.

8.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

The DPDP Act does not contain any such specific protections.

8.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

Yes. The DPDP Act does not prohibit or address the appointment of a single DPO to serve multiple entities. However, such DPO will need to comply with other conditions such as being based in India and also be practically required to be responsible to the Board of Directors or similar governing body of the SDF, as well as act as the point of contact for the grievance redressal mechanism of such SDFs. Therefore, if a DPO is appointed to cover multiple entities, such DPO will need to be able to effectively perform their functions in relation to each such entity covered.

8.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The DPDP Act does not prescribe any specific qualifications for the appointment of a DPO. Practically, any person appointed as the DPO will need to be qualified, experienced and capable of complying with their obligations.

8.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

Please refer to our response to question 8.5 for the responsibilities of a DPO prescribed under the DPDP Act.

8.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

The DPDP Act does not require SDFs to register/notify the appointment of DPO to the DPB or any other authorities.

8.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

The DPDP Act requires that the business contact information of the DPO (if appointed) or a contact person, must be: (i) prominently published on the website or app of the data fiduciary; and (ii) included in every response issued to a data principal in relation to the exercise of their rights contained thereunder. The DPDP Act does not prescribe any specific requirements relating to the placement of the DPO details on its website or app, and accordingly, may be named in a public-facing privacy policy published on its website as well. Further, the details of such DPO will need to be provided in the notice provided to the data principal to obtain their consent.

9 Appointment of Processors

9.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes. Section 7(b) of the DPDP Act mandates a data fiduciary (which includes a business/entity) to engage, appoint, use, or otherwise involve a data processor to process personal data on its behalf only under a valid contract.

9.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The DPDP Act does not prescribe specific formalities or mandatory clauses for agreements to be entered into between a data fiduciary and a data processor. However, given the DPDP Act places the responsibility of the processing undertaken by a data processor on the data fiduciary, it is recommended that the agreement between the data fiduciary and the data processor records the obligations of the data processor, including scope and limits of the processing activities, reasonable security measures to be adopted, personal data breach reporting obligations, etc., and appropriate representations and warranties backed by indemnities are sought.

10 Marketing

10.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

The DPDP Act does not prescribe any specific restrictions on sending of electronic direct marketing. However, it is likely that organisations will need to rely on consent as the basis for processing personal data for marketing purposes. Accordingly,

the notice and consent obligations provided under the DPDP Act will need to be complied with.

10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

The DPDP Act applies to processing of any digital personal data that relates to an individual, regardless of the business context, i.e., the DPDP Act does not differentiate between business-to-consumer and business-to-business context.

10.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

In addition to the notice and consent requirements under the DPDP Act, in the event of sending marketing or promotional messages or calls, the Telecom Commercial Communications Customer Preference Regulations, 2018, issued by the TRAI, prescribe certain requirements such as obtaining prior consent for promotional messages, providing opt-out mechanisms to customers, checking the National Customer Preference Register, etc.

10.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Yes, the DPDP Act has extraterritorial applicability and extends to entities established outside India, if such processing of personal data is in connection with offering goods or services to data principals located within India.

10.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

At the time of writing, there is limited enforcement of the data protection framework envisaged under the SPDI Rules. However, once the DPDP Act is enforced and as the law evolves, we expect that the DPB will be active in enforcement of the notice and consent requirements mentioned thereunder, which will apply to marketing.

10.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

The DPDP Act does not explicitly prohibit purchase of marketing lists or payment of any consideration for acquisition of such lists. However, given that consent is likely to be the primary basis for processing personal data for marketing purposes, it is recommended to ensure, through contractual arrangements, that appropriate consent has been obtained from the data principal by the transferor to share such personal data, as well as for the receiving/transferee entity to process such personal data for marketing purposes, in addition to seeking appropriate representations and warranties backed by indemnities.

10.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Failure to observe compliance under the DPDP Act relating to personal data processed for sending marketing communications may lead to monetary penalties of up to INR 50 crores, with the exact amount of penalty to be determined by the DPB based on factors such as the nature, severity, type of personal data affected, etc.

11 Cookies

11.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

The DPDP Act does not specifically address the use of cookies. If the cookies (or similar technologies) collect/process personal data, then the requirements under the DPDP Act will need to be complied with. For most use cases, we expect consent to be the basis for processing personal data collected through such cookies. Accordingly, data fiduciaries will need to provide appropriate notice and obtain consent as required under the DPDP Act. Further, in case of children's personal data, the prohibitions on tracking or behavioural monitoring of children or targeted advertising directed at children, will need to be adhered to.

Additionally, the IT Act prohibits unauthorised access to computer systems and data. Accordingly, consent may need to be obtained from the owners or authorised users of the computer systems and data in order to place cookie files or use similar technologies on their systems.

11.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

The DPDP Act does not specifically address the use of cookies and therefore, it does not distinguish between different types of cookies. However, to meet the requirements of consent (such as free, specific, etc.) separate consents may need to be obtained depending on the purposes for which the personal data collected through cookies is utilised (such as functional, advertising, etc.).

11.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

At the time of writing, given the DPDP Act is yet to be enforced, there have not been any such reported enforcement actions.

11.4 What are the maximum penalties for breaches of applicable cookie restrictions?

If cookies are used to collect or process personal data of data principals in breach of the requirements prescribed under the DPDP Act, such processing may lead to monetary penalties of up to INR 250 crores depending on the type of non-compliance.

12 Restrictions on International Data Transfers

12.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Section 16 of the DPDP Act allows free cross-border transfer of personal data except to countries notified by the Government of India as restricted/prohibited (this is yet to be notified). In this regard, Rule 12 of the Draft Rules proposes certain restrictions relating to the transfer of personal data to other jurisdictions in the context of SDFs, wherein the Central Government, based on recommendations of a committee it constitutes, may specify certain personal data sets and the traffic data pertaining to its flow that cannot be transferred outside India. Further, as per the Draft Rules, cross-border transfer of personal data by any data fiduciary is proposed to be permitted subject to compliance with conditions prescribed by the Central Government, in respect of making such personal data available to foreign States or entities under their control.

12.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

Any transfer of personal data abroad will need to be in accordance with consent provided by the data principal or based on one of the nine specified legitimate uses, or under one of the exempted grounds provided under Section 17(1) of the DPDP Act, such as for the purpose of enforcement of a legal right or claim, for the purpose of a merger or amalgamation sanctioned by a competent authority, etc. The DPDP Act does not provide any further requirements in relation to cross-border transfer. However, organisations typically enter into data processing agreements recording the details of the transfer and obtain appropriate representations, warranties and indemnities, depending on the role of the transferor and transferee entities.

12.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

There is no requirement under the DPDP Act to obtain any registration/notification or prior approval from the DPB or any other authority for the purpose of transfer of personal data to other jurisdictions.

12.4 Do transfers of personal data to other jurisdictions require a transfer impact assessment? If conducting a transfer impact assessment is only mandatory in some circumstances, please identify those circumstances.

No, there are no such transfer impact assessments prescribed under the DPDP Act. However, as per Section 10 of the DPDP Act, SDFs are required to undertake periodic data protection impact assessments, which may include transfer-related risks.

12.5 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?

There has been no such guidance issued as of the time of writing by any competent authority.

12.6 What guidance (if any) has/have the data protection authority(ies) issued in relation to the use of standard contractual/model clauses as a mechanism for international data transfers?

There has been no such guidance issued as of the time of writing by any competent authority. However, as a matter of practice, and as may be required under foreign laws, many organisations, especially multinational organisations, adopt standard contractual clauses issued by competent authorities under the EU GDPR and other competent foreign authorities in implementing international data transfers.

13 Whistle-blower Hotlines

13.1 What is the permitted scope of corporate whistleblower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

There are no specific whistleblower protection requirements under the DPDP Act. The principal legislation on this subject, the Whistleblower Protection Act, 2014 (“**Whistleblower Act**”), which aims to safeguard individuals reporting corruption or abuse of power by public servants, has not yet been brought into force. However, the Companies Act, 2013, and applicable securities regulations mandate certain classes of companies to establish vigil or whistleblower mechanisms, offering protection against victimisation of employees or directors raising concerns. The mechanism enables reporting of unethical behaviour, suspected fraud, or violations of the company’s code of conduct or ethics policy. Additionally, the RBI’s Master Directions on Frauds (dated July 1, 2016) require commercial banks and select financial institutions to adopt whistleblower policies that encourage reporting of fraudulent activities in accounts and ensure protection for whistleblowers.

13.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Please see our response to question 13.1 above. While the laws discussed above do not prohibit anonymous reporting, the identification of the whistleblower may be required to seek additional clarifications or information from such individuals. Under the Whistleblower Act, identification of the whistleblower is expressly required to prevent abuse of process.

14 CCTV

14.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

No, there are no such registration/notification/prior approval requirements prescribed under the DPDP Act. However, depending on the use case for processing of personal data collected through CCTV, such as where the CCTV is installed in a public place, within a private property, commercial property, etc., the legal basis for such processing may need to be evaluated. As a recommended best practice, there should be an evaluation of reasonable expectation of privacy of an individual and appropriate notices by way of a high visibility sign, etc.

14.2 Are there limits on the purposes for which CCTV data may be used?

Depending on the legal basis for processing personal data captured through CCTV, purpose limitation and retention requirements should be adhered to.

15 Employee Monitoring

15.1 What types of employee monitoring are permitted (if any), and in what circumstances?

One of prescribed legitimate uses (for which consent is not required) includes processing of personal data for the purpose of employment or those related to safeguarding the employer from loss or liability, such as prevention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, classified information or provision of any service or benefit sought by an employee. In such cases, employee monitoring through various means such as CCTV, email and device monitoring, etc., may be permitted.

15.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Please see our response to question 15.1 above.

15.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

The DPDP Act does not prescribe notification to or consultation with representatives of works councils/trade unions/employees.

15.4 Are employers entitled to process information on an employee's attendance in office (e.g., to monitor compliance with any internal return-to-office policies)?

If such processing can be justified under the legitimate use cases described in our response to question 15.1, we believe such employee attendance information may be permitted to be processed. For abundant caution, consent may be sought by organisations for such use cases that may not strictly be justified under the permitted legitimate use.

16 Data Security and Data Breach

16.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Yes, Section 8(4) of the DPDP Act requires every data fiduciary to implement reasonable security measures to prevent personal data breaches. The Draft Rules propose certain minimum-security measures to be implemented, including: encryption; access control; maintenance of logs to monitor, review and detect unauthorised access and take remedial measures; and data backups to mitigate operational disruption caused by compromise in confidentiality or availability of personal data; etc.

16.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Yes, the DPDP Act requires the data fiduciary to intimate the DPB in the event of a personal data breach. As per the Draft Rules, the data fiduciary, upon becoming aware of the personal data breach, must provide to the DPB, without delay, a preliminary notification containing the description of the breach including its nature, extent, timing, location and potential impact. Thereafter, a more detailed intimation needs to be made to the DPB within 72 hours (or within such extended timeline permitted by the DPB) with updated information, including measures implemented or proposed to mitigate risk, findings of the investigation, remedial measures undertaken and intimations given to affected data principals.

16.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Yes, the DPDP Act requires the data fiduciary to intimate the affected data principals in the event of a personal data breach. As per the Draft Rules, the affected data principals must be notified without delay, through their user account or any other mode of communication opted by the data principal, with the details of the nature and extent of the breach, potential consequences for the data principal, the safety measures to be implemented by them to protect their interests, and business contact information of a person who can answer their queries.

16.4 What are the maximum penalties for personal data security breaches?

Under the DPDP Act, failure by a data fiduciary to take reasonable security safeguards to prevent personal data breaches can attract a monetary penalty of up to INR 250 crores.

17 Enforcement and Sanctions

17.1 Describe the enforcement powers of the data protection authority(ies).

- (a) **Investigative powers:** The DPB can initiate inquiries into personal data breaches or non-compliance by data fiduciaries, processors or consent managers. At DPB's discretion, it may also direct the parties concerned to attempt resolution of the dispute through mediation by a mutually agreed mediator, or as provided by any applicable law.
- (b) **Corrective powers:** The DPB may issue binding directions to require remedial or mitigation measures in case of a personal data breach or issue directions to data fiduciaries or consent managers pursuant to an investigation in relation to non-compliance with the DPDP Act. It may also accept voluntary undertakings from parties to ensure compliance, which can include commitments to specific actions or refraining from certain conduct.
- (c) **Authorisation and advisory powers:** The DPB does not currently have explicit authorisation or advisory powers under the DPDP Act.
- (d) **Imposition of administrative fines for infringements of specified legal provisions:** The DPB is empowered to impose monetary penalties of up to INR 250 crores for violations of the DPDP Act, following an opportunity to be heard.
- (e) **Non-compliance with a data protection authority:** Failure to comply with the terms of a voluntary undertaking may lead to enforcement proceedings and penalties under Section 33 of the DPDP Act, following an opportunity to be heard. Any person aggrieved by an order or direction made by the DPB may prefer an appeal before the Appellate Tribunal. An order passed by the Appellate Tribunal will be executable by it as a decree of the civil court.

17.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The DPB has broad powers to issue such directions as it may consider necessary, for the effective discharge of its functions and also direct remedial or corrective measures in case of a personal data breach. Such directions may include a ban on a particular processing activity, if considered necessary by the DPB.

17.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

As the DPDP Act is yet to be enforced and the DPB is yet to be established, we currently do not have any precedents to establish the DPB's approach.

17.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

As discussed under our response to question 3.1, the DPDP Act does have extra-territorial applicability in certain cases.

We will need to see how the enforcement trends evolve once the DPDP Act is notified, in order to establish the manner of enforcement against businesses established abroad. Having noted that, the Indian Supreme Court is hearing a case involving challenge to WhatsApp's privacy policy for violating the right to privacy, in particular, where the policy update of 2021 permits WhatsApp to share data with Facebook and all its group companies for the purposes of commercial advertising and marketing. In this case, the Supreme Court has ordered that in the interim, WhatsApp must publicise that users of WhatsApp who have not yet accepted the privacy policy update of 2021 may continue to use WhatsApp without fear of their accounts being deleted.

18 E-discovery/Disclosure to Foreign Law Enforcement Agencies

18.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Businesses typically evaluate the scope of the request as well as its legal validity, prior to disclosure of personal data. Most contracts under which businesses may have received information may have requirements to inform the transferor regarding such requests to enable them to obtain necessary stay or similar protective orders in respect of such requests, as well as to share only limited information necessary to comply with such requests.

18.2 What guidance has/have the data protection authority(ies) issued on disclosure of personal data to foreign law enforcement or governmental bodies?

There has been no such guidance issued. However, the Draft Rules propose that such transfer is to be permitted subject to compliance with conditions prescribed by the Central Government, in respect of making such personal data available to foreign States or entities under their control.

19 Artificial Intelligence

19.1 Are there any limitations on automated decision-making involving the processing of personal data using artificial intelligence?

No, there are no such requirements. However, the Draft Rules propose that SDFs are required to observe due diligence to verify that algorithmic software deployed by it for hosting, display, uploading, modification, publishing, transmission, storage, updating or sharing of personal data processed by it are not likely to pose a risk to the rights of data principals.

19.2 What guidance (if any) has/have the data protection authority(ies) issued in relation to the processing of personal data in connection with artificial intelligence?

No formal guidance has been issued under the DPDP Act on AI-related personal data processing. However, the MeitY has issued directions to address AI-related harms such as deepfakes. Notably, MeitY's AI Governance Report (dated January 6, 2025) outlines non-binding recommendations for

AI developers and deployers to comply with data protection laws, respect user privacy and implement safeguards like data quality and security-by-design.

20 Trends and Developments

20.1 In your opinion, what enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.

Given the nascency of the DPDP Act, and its impending notification, there have been no notable enforcement trends to report during the previous 12 months.

20.2 In your opinion, what “hot topics” are currently a focus for the data protection regulator?

The DPDP Act is yet to be enforced, and the DPB is yet to be constituted; however, several “hot topics” are already drawing regulatory and stakeholder attention. Some of these include the treatment of cross-border data transfers, with a focus on potential data localisation requirements for SDFs. Another critical area is the processing of children’s data, where the mechanism for obtaining verifiable parental consent is still under debate. Additionally, the use of publicly available personal data, particularly for purposes like profiling, targeted advertising or AI training, is under scrutiny to ensure such usage aligns with the provisions and requirements of the DPDP Act.

Acknowledgments

We would like to extend our sincere gratitude to Prateek Pushkarna and Shruti Agrawal, Associates at AZB & Partners, for their invaluable contributions to this chapter.



Rachit Bahl is a Senior Partner in the Firm's Delhi office with over 20 years of experience advising multinational corporations, including several *Fortune 500* companies, on complex regulatory, policy, and strategic matters. His practice focuses on data protection and privacy, technology law, telecommunications, fintech, and digital business models. He has worked extensively on issues relating to the implementation of global and Indian data protection frameworks, including the Digital Personal Data Protection Act, 2023, and sector-specific privacy obligations. Rachit regularly assists clients in developing cross-border data transfer mechanisms, privacy risk assessments, data breach response protocols, and privacy-by-design integration for digital products and services.

AZB & Partners

AZB House, Plot No A-7 and A-8, Sector 4
Noida 201 301, National Capital Region
India

Tel: +91 120 417 9999
Email: rachit.bahl@azbpartners.com
LinkedIn: www.linkedin.com/in/rachit-bahl-14a502102



Rohan Bagai is a Senior Partner in the Firm's Delhi office with over 18 years of experience and deep expertise in data protection, privacy, and digital business regulation. He regularly counsels domestic and international clients on legal, regulatory, and compliance frameworks relating to data protection and privacy, digital payments, fintech, and e-commerce. Rohan has considerable experience advising on data protection and privacy matters under the Digital Personal Data Protection Act, 2023, the Information Technology Act, 2000, and sectoral guidelines issued by regulators such as the Reserve Bank of India (RBI). His work includes data discovery and mapping, privacy impact assessments, consent and data retention frameworks, cross-border data transfer strategies, and review of vendor and intra-group data processing arrangements.

AZB & Partners

AZB House, Plot No A-7 and A-8, Sector 4
Noida 201 301, National Capital Region
India

Tel: +91 120 417 9999
Email: rohan.bagai@azbpartners.com
LinkedIn: www.linkedin.com/in/rohanbagai



Sumit Ghoshal is a Senior Partner based in the Delhi office with over 18 years of experience advising clients on legal, regulatory, and commercial aspects of e-commerce, digital platforms, technology transactions, and data protection. His practice focuses on supporting businesses in launching and operating digital services in India, including online marketplaces, digital content platforms, and next-generation consumer technology products. He has advised a wide range of clients on structuring and implementing e-commerce models, including website operations, online sale and marketing of products, licensing and registration requirements, and drafting commercial contracts and platform agreements.

AZB & Partners

AZB House, Plot No A-7 and A-8, Sector 4
Noida 201 301, National Capital Region
India

Tel: +91 120 417 9999
Email: sumit.ghoshal@azbpartners.com
LinkedIn: www.linkedin.com/in/sumit-ghoshal-ab2534125



Archana Iyer is a Senior Associate with over nine years of specialised experience in TMT law, with a focus on data protection and artificial intelligence (AI). She advises clients across diverse sectors, including e-commerce, digital products, healthcare, AI, digital advertising, fintech, and telecommunications. Archana has developed deep expertise in India's evolving data protection landscape, particularly under the Digital Personal Data Protection Act, 2023. She supports clients through data discovery, data mapping, and identifying compliance gaps, while recommending actionable compliance roadmaps. Her privacy practice includes reviewing UI/UX for consent mechanisms, drafting or review of SOPs, privacy policies, data retention, and archiving policies, etc.

AZB & Partners

AZB House, Plot No A-7 and A-8, Sector 4
Noida 201 301, National Capital Region
India

Tel: +91 120 417 9999
Email: archana.iyer@azbpartners.com
LinkedIn: www.linkedin.com/in/archana-iyer-22b6a032

AZB & Partners was founded in 2004 with a clear purpose to provide reliable, practical and full-service advice to clients, across all sectors. Having grown steadily since its inception, the Firm now has offices across Mumbai, Delhi, Bangalore, Pune, and Chennai. The Firm has an accomplished and driven team of 650+ lawyers committed to delivering best-in-class legal solutions to help every client achieve their objectives. The Firm works on both advisory and transactional mandates and often in a cross-jurisdictional context.

www.azbpartners.com



Indonesia

ATD Law in association with Mori Hamada



Abadi Abi
Tisnadisastra



Prayoga
Mokoginta



Aloysius Andrew
Jonathan

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The main legislation for personal data protection in Indonesia is Law No. 27 of 2022 on Personal Data Protection (“**PDP Law**”). The PDP Law serves as a comprehensive regulatory framework for personal data processing activities, applicable to all types of businesses, industries and organisations, whether private or public.

While the PDP Law applies to all data processing activities, other sectoral laws and regulations (see questions 1.2 and 1.3) may provide additional/more stringent provisions for specific types of data processing that fall under the scope of such regulations insofar as they do not contradict with the provisions set out under the PDP Law.

Despite the PDP Law’s two-year transitional period having elapsed on 17 October 2024, the Indonesian Government is currently still in the process of drafting the PDP Law’s implementing regulation, and the draft of such regulation was last circulated on 31 August 2023 for public discussion (“**RPP PDP**”). Based on the publicly available version, the RPP PDP will provide extensive elaboration and guidelines on certain aspects stipulated under the PDP Law.

1.2 Is there any other general legislation that impacts data protection?

Yes, there are several other laws that address personal data in various contexts, among others:

- a. Electronic Information and Transaction (“**EIT**”) regulatory framework: Law No. 11 of 2008 on EIT as lastly amended by Law No. 1 of 2024 (“**EIT Law**”), Government Regulation No. 71 of 2019 on the Operation of Electronic System and Transaction (“**GR 71/2019**”), Minister of Communication and Informatic (“**MOCI**”) Regulation No. 5 of 2020 on the Organization of Private Electronic System as amended by MOCI Regulation No. 10 of 2021 (“**MOCI 5/2020**”) and MOCI Regulation No. 20 of 2016 on Data Protection in Electronic System (“**MOCI 20/2016**”).
- b. Law No. 36 of 1999 on Telecommunication (as amended).
- c. Law No. 7 of 1992 on Banking (as amended).
- d. Law No. 17 of 2023 on Health (“**Health Law**”).
- e. Law No. 1 of 2023 on Criminal Code, which stipulates criminal acts pertaining to data, e.g., data falsification and data theft.

1.3 Is there any sector-specific legislation that impacts data protection?

Yes, there are several sector-specific regulations that contain personal data protection provisions, including:

- a. the Financial Services Authority (“**OJK**”) Regulation No. 22 of 2023 on Consumer and Public Protection in The Financial Services Sector (“**OJK Consumer Protection Regulation**”), and its implementing regulation, namely OJK Circular Letter No. 12/SEOJK.07/2014 of 2014 on the Delivery of Information for Marketing of Financial Products and/or Services, which apply to protection of consumers’ personal data within the financial services sector;
- b. the Bank Indonesia (“**BI**”) Regulation No. 3 of 2023 on BI Consumer Protection (“**BI Consumer Protection Regulation**”) and its implementing regulation, namely Members of the Board of Governors Regulation No. 20 of 2023 on the Implementation Procedure of BI Consumer Protection, which apply to the protection of consumers’ personal data within the payment system sector;
- c. the OJK Regulation No. 40 of 2024 on Information Technology-Based Collective Financing Services;
- d. the OJK Regulation No. 3 of 2024 on the Organization of Technological Innovation on the Financial Sector; and
- e. other financial service-specific regulations, such as those that are applicable for digital banks, multi-finance companies, equity crowdfunding and the trading of crypto/digital assets.

1.4 What authority(ies) are responsible for data protection?

Currently, Indonesia is still in the process of establishing a national data protection authority (“**Indonesian DPA**”), as mandated by the PDP Law. Once established, this authority will be the main authority for: (i) formulation and stipulation of policies and strategies for personal data protection; (ii) supervision on the operation of data protection; (iii) enforcement of violations of personal data protection; and (iv) facilitation of alternative dispute resolution.

In the meantime, the role of personal data protection supervision is being carried out primarily by the Ministry of Communication and Digital (“**MOCD**”).¹ Pursuant to MOCD Regulation No. 1 of 2025 on Organization and Work Procedures of MOCD, the role of personal data protection supervision is currently being carried out by the General Directorate of Digital Space Supervision. The General Directorate of Digital

Space Supervision is responsible for formulating and implementing policies related to the supervision of digital space and personal data protection.

For specific sectors such as financial services or payment systems, each sectoral supervisory and regulatory body has the authority to regulate and supervise the data protection-related matters.²

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **“Personal Data”**
Personal data means any data related to identified or identifiable individuals, separately or in combination with other information, directly or indirectly, through an electronic or non-electronic system.
- **“Processing”**
Processing includes activities of data acquisition, collection, analysis, storing, rectification, update, display, announcement, transfer, dissemination, disclosure, erasure and/or disposal.
- **“Controller”**
Controller means any person or corporation, public institution and international organisation acting individually or jointly that determine the purposes and have control over personal data processing activities.
- **“Processor”**
Processor means any person or corporation, public institution and international organisation acting individually or jointly in processing personal data on behalf of the controller.
- **“Data Subject”**
Data subject means an individual whose data are associated with.
- **“Sensitive/Specific Personal Data”**
The PDP Law categorises personal data into general data and specific (sensitive) data, which includes:
 - a. health information and data;
 - b. biometric data;
 - c. genetic data;
 - d. criminal records;
 - e. children’s data;
 - f. personal financial data; and/or
 - g. other data in accordance with provisions of laws and regulations.³
- **“Data Breach”**
Data breach means failure to protect a person’s personal data in terms of confidentiality, integrity and availability of the personal data, including security breaches, whether intentional or unintentional, leading to disposal, loss, alteration, disclosure or unauthorised access to the data which are being transferred, stored or processed.
- **“Transfer”**
Transfer means the assignment, disclosure or making available personal data, both electronically and non-electronically, from one party to another entity.
- **“Profiling”**
Profiling means an activity of identifying a person, including, but not limited to: work history; economic condition; health; personal preferences; interests; reliability; behaviour; location; or movement of the data subject.

3 Territorial and Material Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

Yes, the PDP Law has an extraterritorial coverage. The PDP Law also applies to processing activities outside Indonesian jurisdiction that have legal effect or consequence: (i) within Indonesian jurisdiction; and/or (ii) towards Indonesian data subjects outside Indonesia.

3.2 Do the data protection laws in your jurisdiction carve out certain processing activities from their material scope?

Yes, data processing conducted by individuals for personal or household purposes are not subject to the PDP Law. As a reference, the RPP PDP provides that such activities include: (i) data processing activities that are not part of professional and/or commercial activity; and/or (ii) data processing activities that are not intended for the public.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
Data processing shall be carried out by ensuring that data subjects know the personal data being processed as well as how they are processed. Any information and communication related to personal data processing must also be clear, accessible and easy to understand.
- **Lawful basis for processing**
Data processing activities must be carried out based on the appropriate lawful grounds, namely: (i) lawful consent; (ii) performance of a contract; (iii) legal obligation; (iv) vital interests; (v) duties for public interest; and/or (vi) legitimate interests. Certain sectoral regulations may restrict lawful basis for certain entities. For example, financial service entities are generally more consent centric.
- **Purpose limitation**
The purpose of data processing must be informed and the data processing must be conducted in accordance with such purposes. Data processing purposes must be specified, explicit and legitimate.
- **Data minimisation**
Data collection must be limited to personal data that are relevant to what is necessary for the informed purpose.
- **Proportionality**
The processing of personal data must be conducted in a manner that is only necessary and appropriate to achieve the purposes of data processing, without exceeding its intended scope.
- **Lawful retention**
This principle requires the destruction or erasure of the personal data if the retention period ends or it is requested by the data subject, in accordance with the applicable laws and regulations.
- **Accuracy**
This principle requires the processed data to be accurate and up to date.

- **Integrity, security and confidentiality**
This principle requires the protection of the processed data against unauthorised or unlawful processing activity, including unauthorised access, unauthorised disclosure, unauthorised alteration, misuse, loss or damage of data.
- **Ensuring data subjects' rights**
In carrying out data processing activities, the rights of data subjects must be taken into account and complied with, in accordance with the applicable laws and regulations.
- **Accountability**
This principle requires the processing activities to be carried out in a manner that compliance can be demonstrated.

The PDP regulatory framework through the RPP PDP will further elaborate on several minimum requirements of technical and organisational measures that, in several cases, must be implemented by organisations to ensure adherence to these principles.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to (copies of) data or information about processing**
A data subject is entitled to access and obtain a copy of their personal data. A data subject is also entitled to obtain information on the identity, lawful ground, purpose of request and use of personal data, and accountability of the party requesting the personal data.
- **Right to complete, update and/or rectification of errors or inaccuracies**
A data subject is entitled to rectify errors or inaccuracies of their personal data. A data subject may also complete or update personal data of themselves provided such rectification, completion or update is in accordance with the purpose of data processing.
- **Right to terminate processing, deletion and/or disposal of personal data**
A data subject has the right to terminate, delete and/or dispose of their personal data, in accordance with applicable laws and regulations.
- **Right to object against automated decision-making**
A data subject has the right to object to the processing of their personal data by automated decision-making that result in legal consequences or have a significant impact on the data subject.
- **Right to restrict processing**
A data subject may suspend or restrict data processing proportional to the purpose of data processing.
- **Right to data portability**
A data subject may obtain, utilise and transfer their personal data to another controller, insofar as the system may communicate safely in accordance with the principles provided under the PDP Law.
- **Right to withdraw consent**
A data subject is entitled to withdraw their submitted consent to the data processing.
- **Right to file a lawsuit**
A data subject has the right to file a lawsuit and receive compensation over the violation of their processed personal data.

- **Right to complain to the relevant data protection authority(ies)**
The Indonesian DPA may receive complaints/reports of personal data protection incompliance; a data subject is entitled to complain to the relevant authority in respect of a data protection violation.
The PDP regulatory framework through the RPP PDP would further elaborate on means for which organisations may fulfil the exercise of these rights, along with grounds on which organisations may refuse to fulfil a data subject's request for these rights.

5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

The PDP Law does not expressly regulate this matter. However, in general, collective redress or class action is recognised under Indonesian law.

6 Children's Personal Data

6.1 What additional obligations apply to the processing of children's personal data?

The processing of children's personal data requires the consent of their parent or guardian. As a reference, the RPP PDP requires organisations to verify the consent granted by such children's parent or guardian. Further, based on the EIT Law, electronic system operators ("ESOs") shall provide: (i) information on the minimum age limit of users of its products or services; (ii) a verification mechanism for child users; and (iii) a mechanism for reporting abuse of products, services and features that violate or potentially violate children's rights. Although the age threshold for minors in Indonesia is stipulated differently under different laws and regulations, the RPP PDP stipulates that a child is an individual who is under 18 years old and unmarried.

The Indonesian government is also currently drafting an implementing regulation on the governance of child protection in the organisation of electronic systems. It notably requires ESOs to conduct a data protection impact assessment ("DPIA") for any products, services or features to be used by children, by at least three months prior to the launch of such products/services/features. It also requires ESOs to implement technical and operational measures to ensure the appropriate age of users accessing such products/services/features, as well as to appoint a data protection officer ("DPO"). ESOs are prohibited from conducting profiling of children and collecting precise geolocations of children by default.

7 Registration Formalities and Prior Approval

7.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

The PDP Law does not require organisations to register or notify any governmental body for the data processing activities.
However, if an organisation (Indonesian or offshore) processes personal data through an electronic system (i.e., website or application), such organisation can be considered as

an ESO – and accordingly, is subject to obtain an ESO registration certificate under the EIT regulatory framework. Failure to do so is subject to an administrative sanction in the form of blocking access to the electronic system by the MOCD.

For notification/registration/approval relating to cross-border/international personal data transfer, please see question 12.1 below.

7.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

To obtain an ESO registration certificate, an organisation is required to submit several documents and information which, among others, are related to the personal data that will be processed in the electronic system and information on the location of the data server. Substance-wise, the submission process only requires general information on the aforementioned items.

7.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

See question 7.1 above.

7.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

See question 7.1 above.

7.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

See question 7.2 above.

7.6 What are the sanctions for failure to register/notify where required?

See question 7.1 above.

7.7 What is the fee per registration/notification (if applicable)?

This is not applicable to our jurisdiction.

7.8 How frequently must registrations/notifications be renewed (if applicable)?

Pursuant to MOCI 5/2020, any changes on the information submitted for an ESO registration certificate must be notified to the MOCD.

7.9 Is any prior approval required from the data protection regulator?

This is not applicable to our jurisdiction.

7.10 Can the registration/notification be completed online?

The ESO registration certificate process is completed online through an Online Single Submission system, an integrated electronic system for the implementation of licensing in Indonesia.

7.11 Is there a publicly available list of completed registrations/notifications?

The list of registered domestic and foreign ESOs can be accessed through the following link: <https://pse.komdigi.go.id/pse> (available in the Indonesian language only).

7.12 How long does a typical registration/notification process take?

There is no specific timeline for the ESO certificate registration process. However, in practice, it may take around one to three business days.

8 Appointment of a Data Protection Officer

8.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

An organisation is required to appoint a DPO if the following conditions are met cumulatively:

- the data processing is carried out for the interest of public services;
- the nature, scope and/or purpose of the controller's core activities require regular and systematic monitoring of personal data on a large-scale basis; and
- the core activities of the controller consist of large-scale processing activities of sensitive personal data and/or personal data relating to criminal activities.

A DPO may be appointed from within or outside the organisation, such as a consultant or lawyer, as long as such appointment is made based on professional qualities, expert knowledge, practice of personal data protection and the ability to fulfil the tasks. Further, the RPP PDP provides that the appointment of a DPO must consider the structure, size and need of the organisation.

A more detailed provision on the appointment of a DPO will be further regulated by a technical regulation that will be issued by the Indonesian DPA.

8.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

Violation on the DPO appointment obligation is subject to an administrative sanction stipulated under the PDP Law in the form of: (i) written warning; (ii) temporary suspension of data

processing activity; (iii) erasure or destruction of personal data; and/or (iv) an administrative fine with the maximum amount of two per cent of annual income against the violation variable.

8.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

Although the PDP Law does not expressly stipulate such matters, the RPP PDP provides that organisations must ensure that a DPO shall not be dismissed or penalised in performing their duties in accordance with applicable rules and regulations.

8.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

The PDP regulatory framework does not expressly stipulate this matter. However, pursuant to the RPP PDP, we may anticipate that technicalities of the DPO, including the appointment of a single DPO for multiple entities, would be further regulated by a technical regulation that will be issued by the Indonesian DPA.

8.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The appointment of a DPO must consider professionalism, expert knowledge, data protection experience and ability to fulfil the duties. Based on the RPP PDP, we anticipate that the qualification of a DPO would be regulated under a technical regulation that will be issued by the Indonesian DPA.

Meanwhile, Ministry of Manpower Decision No. 203 of 2023 has provided in detail 19 areas of proficiencies that need to be demonstrated by a DPO, such as the ability to formulate inputs to management, to manage audits in relation to personal data protection work plan, etc.

8.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

A DPO is responsible for:

- a. informing and providing advice to the controller or the processor in order to comply with the provisions of PDP Law;
- b. monitoring and ensuring compliance with the PDP Law and the policies of the controller and processor;
- c. providing advice on assessing the impact of personal data protection and monitoring the performance of the controller and the processor; and
- d. coordinating and acting as a liaison for issues related to the processing of personal data.

Additionally, the RPP PDP expands that a DPO must co-operate with internal parties responsible for data security by providing recommendation and supervision on appropriate technical and organisational security measures and assess their work performance.

8.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

The PDP regulatory framework does not expressly stipulate

this matter. However, we anticipate this matter to be regulated under a technical regulation that will be issued by the Indonesian DPA.

8.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

The PDP Law does not expressly stipulate this matter; however, pursuant to the RPP PDP, the contact information of the DPO must be informed to the data subject.

9 Appointment of Processors

9.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

While the requirements to have an agreement (when an organisation engages a processor) is only implied in the PDP Law, it is required under the RPP PDP, which provides the minimum clauses to be included, such as:

- a. the scope of personal data processing conducted by the processor on behalf of the controller;
- b. the method of personal data processing;
- c. the time period of the personal data processing;
- d. the mechanism for supervision, audit and inspection;
- e. the involvement of another processor, if any; and
- f. the appointment of a communication officer.

9.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

See question 9.1 above.

10 Marketing

10.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

There is no regulation that specifically regulates electronic direct marketing in Indonesia.

In terms of personal data protection aspects, electronic direct marketing activities are subject to the PDP Law and the EIT regulatory framework – for example, adhering to personal data protection principles.

In specific sectors, more stringent rules may apply in the sending of electronic direct marketing. Under the BI Consumer Protection Regulations, the sending of direct marketing can only be carried out from Monday to Saturday, outside public holidays and between 08.00–18.00 local time.

The OJK Consumer Protection Regulations also adopted a similar concept, with additional rules, e.g., (i) stating the purpose of the marketing, and (ii) the content must use simple and plain Indonesian language, contain clear information and include the financial services entity. Further, before a financial service company may use personal data indirectly collected from third parties, it must obtain a written statement from the third party that it has obtained consent to do so and inform the consumer on the source of data collection.

10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

There is no specific provision under Indonesian laws and regulations that separate business-to-business and business-to-consumer marketing.

10.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

In general, question 10.1 also applies to marketing via other means. Indonesia also does not have a specific national opt-out list for direct marketing activities.

10.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?

The PDP Law and the EIT Law both contain extraterritorial provisions. Meanwhile, the Consumer Protection Law applies to foreign business actors outside Indonesian jurisdiction conducting business in Indonesian jurisdiction.

10.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

The MOCD, as the supervisory authority in the EIT sector, is relatively active in enforcement of breaches of the EIT regulatory framework – including related to electronic direct marketing activities. Similarly, the OJK and BI are also actively supervising the financial services and payment system sector, respectively.

Since the Indonesian DPA, once established, will take charge of supervising personal data protection compliance, we anticipate that it will also perform supervision over the personal data protection aspects of marketing activities.

10.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

There is no specific provision regulating the purchase of marketing lists from third parties. However, it must adhere to personal data protection rules and regulations.

In practice, entities may share data by concluding a data-sharing arrangement, given that both entities comply with the rules and requirements set forth by applicable laws and regulations – e.g., establishing the appropriate lawful grounds, informing the purposes of processing, etc.

10.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

The maximum criminal penalty for violation of Article 32 of the EIT Law is maximum imprisonment of nine years and/or a fine of IDR 3 billion, while violation of Article 65 of the PDP Law is subject to maximum imprisonment of five years and/or a fine of IDR 5 billion.

11 Cookies

11.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

There are no specific laws and regulations on cookies and/or other identifier technologies. However, insofar that the cookies contain personal data, it is subject to the relevant personal data protection laws and regulations mentioned herein.

11.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

The current applicable regulatory framework does not distinguish between different types of cookies.

11.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

There is no enforcement in relation to cookies to date.

11.4 What are the maximum penalties for breaches of applicable cookie restrictions?

Depending on the type of breaches, any use of cookies and/or other identifier technologies which violate personal data protection rules may be subject to administrative and/or criminal sanctions under the EIT Law and/or the PDP Law.

12 Restrictions on International Data Transfers

12.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Cross-border data transfer (outside Indonesia) can be carried out under the existence of transfer mechanism/tools (“**Transfer Tools**”) as follows:

- a. If the recipient country has an equivalent or higher standard of personal data protection (adequate countries), it will be assessed by the Indonesian DPA pursuant to the RPP PDP.
- b. In case the previous condition is not met, the transferor must ensure the existence of an adequate and binding personal data protection instrument. Based on the RPP PDP, this may be in the form of: (i) an agreement between the transferor and recipient country; (ii) a Standard Contractual Clause (“**SCC**”) that will be issued by the Indonesian DPA; or (iii) a Binding Corporate Rule for a group of companies that must be approved by the Indonesian DPA.
- c. In case the previous conditions are not met, the transferor must obtain the data subjects’ consent. This may only be applicable in limited circumstances as the RPP PDP imposes strict conditions on the use of consent for the transfer of personal data overseas.⁴

Furthermore, the EIT regulatory framework adds another requirement in conducting cross-border data transfer through an electronic system. Article 22 of MOCI 20/2016 requires a

cross-border data transfer to be reported (before and after the transfer), by submitting information such as: (i) the designated country and recipient; (ii) the date of the transfer; and (iii) the purpose of the transfer. The regulation does not provide a specific time period for the reporting, which in practice is submitted annually using the form provided by the MOCD.

It should be noted that certain sectors may have more stringent requirements for international data transfer. For example, the Health Law requires that the transfer of personal data in health information system may only be conducted for a specific and limited purpose and based on approval of the central government, which will be further elaborated in the implementing regulation of the Health Law.

12.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

In addition to the Transfer Tools mentioned in question 12.1, the cross-border data transfer activities must also be carried out in compliance with the principles and rules set out under the PDP Law, the EIT Law and/or the relevant sectoral regulations (as may be applicable).

12.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

See question 12.1.

12.4 Do transfers of personal data to other jurisdictions require a transfer impact assessment? If conducting a transfer impact assessment is only mandatory in some circumstances, please identify those circumstances.

The PDP Law does not govern this matter. However, if we refer to the RPP PDP, such data transfer impact assessment must be carried out by organisations who wish to conduct international data transfer. Please note that the RPP PDP stipulates that further elaboration on data transfer impact assessment will be provided in the technical regulation that will be issued by the Indonesian DPA.

12.5 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?

To date, there is no guidance issued by the authority on this matter.

12.6 What guidance (if any) has/have the data protection authority(ies) issued in relation to the use of standard contractual/model clauses as a mechanism for international data transfers?

To date, the Indonesian DPA has not yet been established, and

as such no guidance has been issued on this matter. However, the RPP PDP provides the clauses that must be governed under the SCC: (i) basis of data processing; (ii) clause on personal data protection; (iii) notification obligation on data breach; and (iv) obligation to conduct due diligence on the recipient of personal data transfer.

13 Whistle-blower Hotlines

13.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

There is no specific law on corporate whistle blowing. The existing regulatory framework only governs a whistle-blowing process within the context of a formal investigation process, witness protection and mostly related to criminal proceedings. Meanwhile, a corporate whistle-blower system/process is commonly implemented based on internal policy/regulation of the company itself. The scope of a corporate whistle-blower system mainly relates to corruption and/or general compliances.

13.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

This may be subject to each company's internal policy on a whistle-blower system. However, it is common for the company to encourage the disclosure of the identity of the reported party – while at the same time provide a protection towards the confidentiality of the whistle blower.

14 CCTV

14.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

In addition to the principles and rules set forth by the PDP Law and the EIT Law, the PDP Law stipulates the use/instalment of CCTV in public places and/or public service facilities to only be carried out under the following conditions (letters b and c are exempted if the purpose is for the prevention of criminal action and law enforcement):

- a. for the purpose of security, disaster prevention and/or traffic management or collection, analysis and regulations of traffic information;
- b. display information stating that CCTV has been installed in the area; and
- c. not used to identify a person.

Any use/instalment of CCTV in private premises (e.g., an office or meeting room) shall comply with the general principles and rules under the PDP Law and the EIT Law – for instance, establishing the appropriate lawful grounds, adhering to the data minimisation principle, informing the purposes of processing, and so on.

As a reference, the RPP PDP further provides that organisations must produce clear and concise information within

the area covered by the CCTV, indicating the operation of such devices as well as the contact information of the person in charge of operating the CCTV. Such information must be placed in the entrance of a closed space or in an easily readable/accessible position.

14.2 Are there limits on the purposes for which CCTV data may be used?

See question 14.1.

15 Employee Monitoring

15.1 What types of employee monitoring are permitted (if any), and in what circumstances?

There is no specific provision and/or guidelines on this matter. Generally, it is permitted if it complies with personal data protection regulations. In practice, common employee monitoring methods that are implemented are the instalment of CCTV in an office room, monitoring tools used in office devices, etc.

15.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

The general applicable requirement under the PDP Law is to establish the appropriate lawful ground to conduct the employee monitoring activities – whether it is based on employment contract or legitimate interest. However, it may be difficult to obtain lawful consent that is freely given in an employment–employer relationship. In practice, employers are commonly providing notice/information at the outset, i.e., when the monitoring tool is first introduced or at the signing of an employment contract.

15.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

A company may have to consult the labour union if the company regulation or collective labour agreement requires the company to do so. As a reference, a collective labour agreement is required to include rights and obligations of both the employer and the employees. Although uncommon, such rights and obligations may include the requirement of conducting consultation or notifying the labour union for certain specific matters, such as the introduction of employee monitoring initiatives.

15.4 Are employers entitled to process information on an employee's attendance in office (e.g., to monitor compliance with any internal return-to-office policies)?

There are no provisions that prohibits an employer from processing an employee's attendance in office. Such purposes are permitted so long as they are carried out in accordance with personal data protection regulations as with any other personal data processing activities.

16 Data Security and Data Breach

16.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

The controller and processor are required to protect and ensure the security of the processed personal data. This shall be achieved through:

- preparing and implementing organisational and technical measures to protect personal data from disruption in the data processing;
- determining the security level of personal data by considering the nature and risks of the processed personal data; and
- using a security system for the processed personal data and/or processing personal data using an electronic system in a reliable, secure and responsible manner.

As a reference, the RPP PDP further elaborates that in terms of security of personal data, organisations shall establish organisational technical measures and determine the level of security by considering the nature and the risk of personal data. Further, organisations are required to conduct gap analysis between the formulated organisational technical measures and the actual implementation of the measures.

16.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

If a data breach occurs, the controller is required to submit a written notification to the affected data subjects and the Indonesian DPA no later than three days from the occurrence of the data breach. In certain circumstances, the data breach shall also be notified to the public if it disturbs public services and/or has a material impact on the public interest. Pursuant to the PDP Law, the notification shall contain the following items:

- the disclosed data;
- the time and technical reason of the data breach; and
- the remedy measure carried out by the controller.

Under the RPP PDP, a data breach notification is exempted if it does not result in the disclosure of personal data. Based on the RPP PDP, the notification timeframe is no later than three days after the organisation discovers the data breach certainly, properly and reasonably based on internal documentation of the organisation. Further, the RPP PDP adds a condition for the obligation to also notify the public of data breach, i.e., when the controller cannot ensure that the data subject can directly receive the data breach notification.

Under the EIT regulatory framework, there is a requirement for the ESO to notify any security incident to the law enforcement authorities and relevant ministry/supervisory, pursuant to GR 71/2019. Such security incident is only applicable in the event of failure or disturbance of an electronic system caused by outsiders and resulting in a serious risk to the electronic system. In addition, the ESO may electronically notify the data subject upon their consent, pursuant to MOCI Reg. 20/2016.

16.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

See question 16.2.

16.4 What are the maximum penalties for personal data security breaches?

Failure in ensuring the security and confidentiality of the processed personal data is subject to the following administrative sanctions:

- a. a written reprimand;
- b. the temporary suspension of the data processing activity;
- c. the erasure or destruction of personal data; and/or
- d. an administrative fine in the maximum amount of two per cent of the annual income or annual receipt of the violation variable.

In regard to the calculation of administrative fines, the RPP PDP provides that the violation variables in determining the fine are, among others: (i) the duration of the violation; (ii) negative impact of the violation; (iii) scale of the organisation's business; and (iv) the organisation's ability to pay the fines.

17 Enforcement and Sanctions

17.1 Describe the enforcement powers of the data protection authority(ies).

- (a) **Investigative powers:** The Indonesian DPA is authorised to carry out investigation in relation to a personal data protection breach allegation.
- (b) **Corrective powers:** The Indonesian DPA is authorised to order an organisation to take corrective measures as a follow up to supervisory measures.
- (c) **Authorisation and advisory powers:** The Indonesian DPA oversees formulation and stipulation of policies and strategies for personal data protection, which shall become the guideline for data subjects, controllers and processors.
- (d) **Imposition of administrative fines for infringements of specified legal provisions:** The Indonesian DPA is authorised to impose administrative sanctions, including fines for non-compliance with personal data protection regulations.
- (e) **Non-compliance with a data protection authority:** The Indonesian DPA may impose administrative sanctions in the event of any non-compliances to personal data protection, as mentioned above.

17.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

Yes, temporary suspension of data processing is one of the administrative sanctions that may be imposed because of a personal data protection breach. Such temporary suspension does not require a court order under the PDP Law.

17.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

As mentioned in question 1.4, while the Indonesian DPA has yet to be established, the MOCD is the primary supervisory authority in connection with data protection issues. In this case, during recent data breach incidents in Indonesia (public and private institutions), the MOCD summoned the relevant institutions to seek clarification on the incidents. However, there are no publicly announced sanctions that were imposed by the MOCD against such relevant institutions.

17.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

The MOCD, as the current data protection supervisory authority in Indonesia, has the authority to exercise its power against organisations outside Indonesian jurisdiction since the EIT Law has extraterritorial provision – for example, by imposing administrative sanctions or blocking access to the electronic system operated by such offshore organisation. However, as at the time of writing, we have not seen the MOCD exercise its power against an organisation outside Indonesian jurisdiction due to a personal data protection violation.

Additionally, in theory, the to-be-established Indonesian DPA will also have similar power against offshore organisations due to the extraterritorial provision stipulated under the PDP Law.

18 E-discovery/Disclosure to Foreign Law Enforcement Agencies

18.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Indonesian laws and regulations are silent on this matter. However, under the PDP Law, the Indonesian DPA is authorised to cooperate with the personal data protection agency of other countries to settle allegations of cross-border personal data protection violation. Furthermore, the obligation for a controller to keep the confidentiality of the processed personal data may be exempted for the interest of the law enforcement process. Therefore, a foreign request for disclosure may be exercised insofar as it is for law enforcement purposes.

18.2 What guidance has/have the data protection authority(ies) issued on disclosure of personal data to foreign law enforcement or governmental bodies?

To date, there is no guidance issued by any authority on this matter.

19 Artificial Intelligence

19.1 Are there any limitations on automated decision-making involving the processing of personal data using artificial intelligence?

Generally, although the PDP Law does not provide any specific

provision on the processing of personal data by artificial intelligence, such limitation falls under the right for a data subject to object against processing from automated decision making which has a legal or significant impact towards the data subject.

In addition, the PDP Law also classifies the processing of personal data using new technology as high-risk data processing, which entails the requirement to conduct a DPIA. As a reference, RPP PDP specifically considers the use of artificial intelligence as new technology in the processing of personal data.

19.2 What guidance (if any) has/have the data protection authority(ies) issued in relation to the processing of personal data in connection with artificial intelligence?

The MOCD has issued Circular Letter No. 9 of 2023 on Artificial Intelligence Ethics, which outlines the ethical guidelines in the development of artificial intelligence. While the nature of the circular letter is very general, it does mention that the organising of artificial intelligence must ensure the protection of personal data as required by laws and regulations.

Additionally, on 4 December 2023, the OJK issued the Code of Ethics Guideline on Responsible and Trustworthy Artificial Intelligence in the Financial Technology Industry as a sector-specific guideline to provide a standard for the use of artificial intelligence by financial technology companies. It requires financial technology companies to use data in compliance with personal data protection regulations, especially regarding automated processing.

20 Trends and Developments

20.1 In your opinion, what enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.

Although the transitory period of the PDP Law elapsed on 17 October 2024, the Indonesian DPA has not yet been established. As such, we observed that there are no recent major enforcement actions as the MOCD is focusing on the issuance of the RPP PDP, as well as the establishment of the Indonesian DPA. In addition, although the OJK and BI have added more

personal data protection provisions within newly issued sectoral regulations, such as the new OJK Regulation No. 40 of 2024 on Information Technology-Based Joint Funding Services, there have been no recent updates of regulation/trends from the central government.

However, a major data breach throughout 2024, which mainly affects government services, has raised awareness to the urgency of stronger personal data protection enforcement. Once the Indonesian DPA is established, we expect stricter enforcement actions and penalties.

20.2 In your opinion, what “hot topics” are currently a focus for the data protection regulator?

Although the RPP PDP was expected to be issued by the end of the transitory period of the PDP Law, such has not occurred. As of February 2025, the MOCD has stated that the RPP PDP is in its fourth harmonisation process and is expected to be issued in the near future. There is reportedly a strengthening of the responsibility of controllers and data subject rights.

In addition, the draft implementing government regulation on online child protection has also been released to the public. It outlines the responsibilities of ESOs in managing online products, services or features to oversee child protection governance within electronic systems, including child personal data.

Endnotes

- 1 The MOCD is the continuation of the MOCI under the current presidential administration since October 2024.
- 2 Referencing the RPP PDP, when the Indonesian DPA is established, it will have the authority to coordinate supervision with such sectoral supervisory and regulatory bodies.
- 3 As a reference, the RPP PDP stipulates that other data may be considered as specific data if its processing may result in discrimination, material/immaterial losses or other unlawful impacts to the data subject.
- 4 Consent may be used under the conditions that: (i) it is a non-recurring data transfer; (ii) it is involving only a limited data subject; (iii) the transfer is required to fulfil a purpose that does not set aside the rights of the data subject; and (iv) the organisation has assessed the risk and informed the data subject and the Indonesian DPA.



Abadi Abi Tisnadisastra's practice covers a broad range of corporate and commercial areas, including M&A, restructuring, joint ventures and foreign investment. He has been involved in numerous cross-border acquisitions and investments in companies from various industries including banking, financial services, manufacturing, information technology, e-commerce and financial technology (Fintech). He also advises foreign investors on operations, corporate governance and legal compliance, advising, whether at the outset of their investment or in connection with the compliant functioning of their ongoing businesses.

Abi is recognised for his in-depth knowledge of financial services and information technology sectors, having advised local and multinational financial institutions (multi-finance, insurance and venture capital companies), tech players, and investors in investing and consolidating operations in Indonesia. He is familiar with the business dynamics in the financial sectors and technology area and is frequently involved in deals, advising multinational and local investors on operations and opportunities in Indonesia.

ATD Law in association with Mori Hamada

Treasury Tower 2F, SCBD, Lot 28 District 8
Jl. Jend. Sudirman Kav. 52-53, Senayan, Kebayoran Baru
Jakarta Selatan, Jakarta 12190
Indonesia

Tel: +62 811 183 700
Email: abadi.t@morihamada.com
LinkedIn: www.linkedin.com/in/abaditisnadisastra



Prayoga Mokoginta specialises in advising on tech-related legal matters. While he handles a variety of areas of legal practice, Yoga mainly focuses his practice on representing Indonesian and multinational clients in M&A transactions, personal data protection/data privacy, technology, fintech and payment systems, e-commerce and general corporate legal matters.

He has an in-depth understanding of regulatory frameworks as well as extensive industry best-practice knowledge in the field of personal data protection and tech-industry. Yoga has also authored multiple international publications on such topics, notably, *International Comparative Legal Guide – Data Protection 2024* as well as *Lexology – Due Diligence for Tech M&A in Indonesia 2024*.

He is a licensed lawyer to appear before the Indonesian courts. He holds a Bachelor of Law (S.H.) degree from Gadjah Mada University, Indonesia, and a Master of Laws (LL.M.) degree from Tilburg University (majoring in Law and Technology, with focus on Personal Data Protection).

ATD Law in association with Mori Hamada

Treasury Tower 2F, SCBD, Lot 28 District 8
Jl. Jend. Sudirman Kav. 52-53, Senayan, Kebayoran Baru
Jakarta Selatan, Jakarta 12190
Indonesia

Tel: +62 821 2528 8330
Email: prayoga.m@morihamada.com
LinkedIn: www.linkedin.com/in/noor-prayoga-mokoginta-015875aa



Aloysius Andrew Jonathan specialises in personal data protection/data privacy compliance, fintech, payment services, e-commerce regulations and other tech-related legal matters. Andrew also has experience in advising clients on employment, anti-bribery/corruption and general corporate compliance issues, as well as assisting multinational clients in conducting internal investigations and cross-border M&A.

Prior to joining ATD Law, Andrew previously assisted as an intern at one of the reputable law firms in Indonesia that specialises in dispute and arbitration matters. Andrew holds a Bachelor's degree in law (S.H.) from Universitas Prasetiya Mulya. Andrew is fluent in both English and Bahasa Indonesia.

ATD Law in association with Mori Hamada

Treasury Tower 2F, SCBD, Lot 28 District 8
Jl. Jend. Sudirman Kav. 52-53, Senayan, Kebayoran Baru
Jakarta Selatan, Jakarta 12190
Indonesia

Tel: +62 811 1923 4049
Email: andrew.j@morihamada.com
LinkedIn: www.linkedin.com/in/alloysiusandrewjonathan

ATD Law is an Indonesian law firm specialising in corporate commercial work, serving both local and international clients. The firm is strategically allied with Mori Hamada, a top-tier Japanese law firm with offices in China, Japan, Myanmar, Singapore, Thailand, Vietnam and the United States. In the Philippines, Mori Hamada has established a strategic relationship with Tayag Ngochua & Chu. This affiliation allows ATD Law to leverage Mori Hamada's extensive regional network and expertise, providing distinctive and excellent services to all clients.

ATD Law offers a comprehensive range of corporate commercial practices, including M&A, foreign direct investment, banking and finance, real estate, employment, capital markets and other corporate practices.

The firm also has specialised areas of legal expertise in technology, media, and telecommunications (TMT), financial technology (Fintech), and personal data protection and privacy.

www.atdmorihamada.com

ATD LAW
in association with
MORI HAMADA

Ireland

Byrne Wallace Shields LLP



Victor Timon



Zelda Deasy



Seán O'Donnell



Jane O'Grady

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

Since 25 May 2018, the principal data protection legislation in the EU has been Regulation (EU) 2016/679 (the “**General Data Protection Regulation**” or “**GDPR**”). The GDPR repealed Directive 95/46/EC and has led to increased (though not total) harmonisation of data protection law across the EU Member States. The Data Protection Act 2018, as amended (the “**DPA 2018**”) transposes the GDPR into national law in Ireland. The former Data Protection Acts 1988 to 2003 still apply in certain circumstances, such as to the processing of personal data for the purposes of safeguarding the security of the State.

1.2 Is there any other general legislation that impacts data protection?

The European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011, as amended (the “**ePrivacy Regulations**”), transpose Directive 2002/58/EC (the “**ePrivacy Directive**”) into law. The ePrivacy Regulations outline specific rules with regard to the use of cookies, marketing communications and security of electronic communications networks and services. The ePrivacy Regulations were amended by the European Union (Electronic Communications Code) Regulations 2022, which broadened the range of service providers falling within the scope of the legislative requirements. The EU Commission has officially withdrawn its proposal for a new ePrivacy Directive. EU Directive 2016/680 specifically regulates the processing of data by police and criminal justice authorities in the EU, such as *An Garda Síochána*, the Irish police force. The Directive requires the data collected by law enforcement authorities to be processed lawfully and fairly.

1.3 Is there any sector-specific legislation that impacts data protection?

The Data Sharing and Governance Act 2019 (the “**DSGA**”) regulates the sharing of personal data within the public sector. It: (i) regulates the sharing of information, including personal data, between public bodies; (ii) provides for the establishment of base registries and implements the Personal Data

Access Portal; and (iii) establishes the Data Governance Board, which is tasked with overseeing compliance, setting standards and promoting best practices in data governance across public entities.

Regulation (EU) 2022/2065 on a Single Market for Digital Services (the “**Digital Services Act**” or “**DSA**”) came into effect in November 2022. The DSA applies to certain entities that provide an online “intermediary service” within the EU, and it builds on some of the well-established themes underpinning the GDPR. The DSA is enforced by the European Commission and “Digital Services Coordinators”, to be designated by each Member State. Ireland has designated *Coimisiún na Meán* (“**CNM**”) as the Irish Digital Services Coordinator and the Competition and Consumer Protection Commission as a competent authority for online marketplaces. In the event of non-compliance with the DSA, service providers could receive fines of up to 6% of their annual global turnover.

The Digital Markets Act (“**DMA**”) came into effect on 1 November 2022 and regulates designated “gatekeepers” of “core platform services” from imposing unfair conditions on businesses and end users, and ensures the openness of important digital services. The DMA applies to companies that exceed certain financial and market share thresholds and operate in certain digital sectors, including advertising services, online search engines, social networking services, online intermediary services, app stores, certain messaging services, virtual assistants, web browsers and operating systems.

The Health Research Regulations 2018 (as amended in 2021) provide suitable and specific measures for the processing of personal data for the purposes of health research. They address issues such as explicit consent to provide protection of the rights of research participants.

The Policing, Security and Community Safety Act 2024, was signed into law on 7 February 2024, and empowers *An Garda Síochána*, the Authority (*An tUdarás Póilíneachta agus Sábháilteachta Pobail*), and the Police Ombudsman to share data, including personal data, with other agencies to perform their functions.

1.4 What authority(ies) are responsible for data protection?

Each EU Member State appoints a dedicated national supervisory authority which is responsible for enforcement and oversight of data protection legislation within its jurisdiction. The Data Protection Commission (“**DPC**”) is the national competent authority for the regulation and enforcement of the GDPR, the DPA 2018 and the ePrivacy Regulations in Ireland.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **“Personal Data”** means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- **“Processing”** means any operation or set of operations that is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- **“Controller”** means the natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data.
- **“Processor”** means a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller.
- **“Data Subject”** means an identified or identifiable natural person.
- **“Sensitive Personal Data”/“Special Categories of Personal Data”** are personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life and sexual orientation, genetic data or biometric data.
- **“(Personal) Data Breach”** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
- **“Identified or identifiable natural person”** means a natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- **“Consent”** means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
- **“Cross-border Processing”** means either: (i) processing of personal data that takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the EU where the controller or processor is established in more than one Member State; or (ii) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the EU, but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

3 Territorial and Material Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The GDPR applies to businesses that are established in any EU Member State, and that process personal data (both as a controller or processor, and regardless of whether or not the processing takes place in the EU). The GDPR also applies to businesses outside the EU if they (either as controller or processor) process the personal data of EU residents in relation to: (i) the offering of goods or services (whether or not in return for payment) to EU residents; or (ii) monitor the behaviour of EU residents (to the extent that such behaviour takes place in the EU).

3.2 Do the data protection laws in your jurisdiction carve out certain processing activities from their material scope?

The GDPR applies where a controller or processor has an establishment in any EU Member State, and they process personal data in the context of that establishment, whether or not the processing takes place in the EU or not.

However Article 2(2) sets out restrictions on the material scope of personal data processing that will not be subject to the GDPR.

Such exempted processing includes processing in the course of an activity that falls outside the scope of Union law, by a natural person in the course of a purely personal or household activity, where it is done by a competent authority for the purposes of prevention, investigation, detection or prosecution of criminal offences.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
Controllers must process personal data in a transparent manner and are obliged to furnish data subjects with certain minimum information regarding the collection and processing of their personal data. This information should be concise, transparent, intelligible and in an easily accessible form, and use clear and plain language.
- **Lawful basis for processing**
Controllers must rely on one of six permitted lawful bases when processing personal data: (i) the consent of the data subject; (ii) necessity for the performance of a contract with the data subject; (iii) compliance with a legal obligation of the controller; (iv) necessity for the protection of the vital interests of the data subject or another natural person; (v) necessity for the performance of a task carried out in the public interest or an official function vested in the controller; and (vi) necessity for the legitimate interests of the controller or a third party, except where those interests are overridden by the interests or rights and freedoms of the data subject.
The processing of special-category personal data is generally prohibited with 10 exceptions provided for in

the GDPR where processing is permitted, such as: (i) with the consent of the data subject; (ii) where processing is necessary for the establishment, exercise or defence of a legal claim; or (iii) where processing is necessary to protect the vital interests of the data subject.

- **Purpose limitation**

Personal data must only be collected for specified, explicit and legitimate purposes and not be further processed in a manner that is incompatible with those purposes. Where a controller wishes to further process the personal data in a manner that is incompatible with the original purposes of collection, the controller must inform the data subject of the further processing and rely on an appropriate lawful basis for processing.

- **Data minimisation**

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed.

- **Proportionality**

Personal data must be processed in a manner which is proportionate to the purpose of the processing. This requires that the advantages achieved by the processing, which may limit the rights of the data subject, must not be outweighed by the disadvantages of exercising the right to process.

- **Retention**

Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods solely for archiving purposes in the public interest, for scientific or historical research purposes or statistical purposes.

- **Accuracy**

Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

- **Integrity and confidentiality**

Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

- **Accountability**

The controller is responsible for, and must be able to demonstrate, compliance with the data protection principles set out above.

- **Fairness**

This principle is not defined in the GDPR; however, the European Data Protection Board (“EDPB”) has stated that it means personal data must not be “processed in a way that is detrimental, discriminatory, unexpected or misleading to the data subject”. Data subjects should, therefore, be sufficiently informed as to how their personal data will be processed.

subject’s personal data: (i) confirmation of whether, and where, the controller is processing the data subject’s personal data; (ii) information about the purposes of the processing; (iii) information about the categories of data being processed; (iv) information about the categories of recipients with whom the data may be shared (note that the Court of Justice of the EU ruled in the *PostAG* (Case C-154/21) that the data subject is entitled to request the actual identities of recipients (not merely the categories) unless this is impossible); (v) information about the period for which the data will be stored (or the criteria used to determine that period); (vi) information about the existence of the rights to erasure, rectification, restriction of processing and to object to processing; (vii) information about the existence of the right to complain to the relevant data protection authority; (viii) where the data were not collected from the data subject, information as to the source of the data; and (ix) information about the existence of, and an explanation of the logic involved in any automated processing that has a significant effect on the data subject.

The data subject may request a copy of the personal data being processed. The copy should include, *inter alia*, the purposes of processing, the categories of personal data processed and the envisaged period for which the personal data will be stored. This right must not adversely affect the rights and freedoms of others.

- **Right to rectification of errors**

Data subjects may oblige controllers to rectify inaccurate personal data concerning them without undue delay. Rectification includes the completion of incomplete personal data, which may be updated by providing a supplementary statement.

- **Right to deletion/right to be forgotten**

Data subjects have the right to erasure of their personal data without undue delay if: (i) the data are no longer needed for their original purpose (and no new lawful purpose exists); (ii) the lawful basis for the processing is the data subject’s consent, the data subject withdraws that consent, and no other lawful basis applies; (iii) the data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing; (iv) the data have been processed unlawfully; (v) erasure is necessary for compliance with EU law or national data protection law; or (vi) the data have been collected in relation to the offer of information society services.

- **Right to object to processing**

Data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data where the basis for that processing is either public interest or legitimate interests of the controller. The controller must cease such processing unless it demonstrates compelling legitimate grounds for the processing that override the interests, rights and freedoms of the relevant data subject or requires the data in order to establish, exercise or defend legal rights.

- **Right to restrict processing**

Data subjects have the right to restrict the processing of personal data, which means that the data may only be held by the controller, and may only be used for limited purposes if: (i) the accuracy of the data is contested (and only for as long as it takes to verify that accuracy); (ii) the processing is unlawful and the data subject requests restriction (as opposed to exercising the right to erasure);

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to (copies of) data/information about processing**

A data subject has the right to obtain from a controller the following information in respect of the data

(iii) the controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights; or (iv) verification of overriding grounds is pending, in the context of an erasure request.

- **Right to data portability**
Data subjects have a right to receive a copy of their personal data in a commonly used machine-readable format, and to transfer their personal data from one controller to another or have the data transmitted directly between controllers.
- **Right to withdraw consent**
A data subject has the right to withdraw their consent at any time and must be informed of this right prior to giving consent. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. It must be as easy to withdraw consent as it is to give it.
- **Right to object to marketing**
Data subjects have the right to object to the processing of their personal data for the purposes of direct marketing, including profiling and to opt out of direct marketing communications.
- **Right protecting against solely automated decision-making and profiling**
Data subjects have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects that concern (or similarly significantly affect) them. This right is restricted where the solely automated decision: (i) is necessary for entering into, or the performance of, a contract between the data subject and controller; (ii) is authorised by EU or Member State law to which the controller is subject (and which contains suitable measures to safeguard the data subject's rights); or (iii) is based on the data subject's explicit consent.
- **Right to complain to the relevant data protection authority(ies)**
Data subjects have the right to lodge complaints concerning the processing of their personal data with the DPC if the data subjects live in Ireland or the alleged infringement occurred in Ireland.
- **Right to compensation**
Section 117 of the DPA 2018 permits an individual to seek compensation for damage caused as a result of the infringement of data protection laws. Damage includes material and non-material damage. The interpretation of "non-material damage" has been the subject of a number of decisions of the CJEU.
A Supreme Court decision is awaited with regard to whether prior authorisation is required from the Injuries Resolution Board (which is the statutory body that assesses the value of an individual's personal injury claims) where a plaintiff is seeking damages for mental distress. This is expected to have a significant impact on a number of cases currently before the Irish Courts.

5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

Yes, in line with Article 80 of the GDPR, the data subject shall have the right to mandate a not-for-profit body, organisation

or association which has been properly constituted in accordance with the laws of a Member State.

6 Children's Personal Data

6.1 What additional obligations apply to the processing of children's personal data?

The GDPR and the DPA 2018 apply to children and adults equally. Under Section 29 of the DPA 2018, a child is defined as a person under the age of 18 years. Sections 30 to 33 of the DPA 2018 relate specifically to children and relate to the micro-targeting and profiling of children, the consent of a child in relation to information society services, codes of conduct in relation to children and a child's right to be forgotten. Section 30, which relates to the micro-targeting and profiling of children, has not yet been commenced.

The age of digital consent in Ireland has been specified as 16 and online providers must make "reasonable efforts" to verify that a person with parental responsibility has consented to the processing of a child under the age of 16's personal data on their behalf, where consent is the legal basis relied upon for that processing.

In December 2021, the DPC published Fundamentals for a child-orientated approach to data processing, which introduced child-specific data protection interpretative principles and recommended measures to enhance the level of protection afforded to children when processing their personal data.

The DSA was signed into law in Ireland in February 2024 and there is a strong focus in the DSA on better protection for children from online harm.

The Online Safety and Media Regulation Act, 2022 (the "2022 Act") was largely enacted in December 2022 and aims to regulate the provision of content and prevent harmful content, though non-traditional media, ranging from social media to online gaming. The 2022 Act aims to create a safer online environment, in particular by addressing the causes of cyber bullying, self-harm or suicide, and material that promotes nutritional deprivation. The 2022 Act also provides for the establishment of CNM, whose remit includes the implementation of a new regulatory framework, as well as holding designated online services to account through legally binding online safety codes. On 21 October 2024, CNM published the Online Safety Code, which sets binding rules for video-sharing platforms in order protect users, especially children, from harmful content.

7 Registration Formalities and Prior Approval

7.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

There are no registration requirements for controllers or processors in Ireland. Under section 88 of the DPA 2018, all organisations that have appointed a Data Protection Officer ("DPO") pursuant to the GDPR, are required to notify the contact details to the DPC, which holds a register of DPOs. A controller is obliged to publish the contact details of the DPO so that it is easily accessible to data subjects.

7.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

This is not a requirement in Ireland.

7.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

This is not a requirement in Ireland.

7.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

Only registration of the DPO is required.

7.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

The entity's name, address, email, telephone number and URL, and the DPO's name, email address and telephone number.

7.6 What are the sanctions for failure to register/notify where required?

No such sanctions apply.

7.7 What is the fee per registration/notification (if applicable)?

No fee applies.

7.8 How frequently must registrations/notifications be renewed (if applicable)?

Notification of change of a DPO should be notified to the DPC without delay.

7.9 Is any prior approval required from the data protection regulator?

Where a controller determines, by way of Data Protection Impact Assessment ("DPIA") that the intended processing would result in a high risk to the data protection rights of individuals, in the absence of mitigation measures, they must consult with the DPC.

7.10 Can the registration/notification be completed online?

Registration of a DPO can be undertaken through the DPC's online form for this purpose.

7.11 Is there a publicly available list of completed registrations/notifications?

There is no publicly available list of completed DPO registrations.

7.12 How long does a typical registration/notification process take?

The registration of the DPO can be completed in a matter of minutes on the DPC website.

8 Appointment of a Data Protection Officer

8.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

A DPO must be appointed in the following circumstances: (i) when processing is conducted by a public authority or body, excluding courts in their judicial role; (ii) when the primary activities of the controller or processor involve processing operations that, due to their nature, extent and/or purposes, necessitate regular and systematic monitoring of a large number of data subjects; or (iii) when the primary activities of the controller or processor involve processing on a large scale of special category data and personal data concerning criminal convictions and offences.

Apart from these scenarios, associations and other bodies representing groups of controllers or processors may choose (or be legally required under the laws of their Member State) to appoint a DPO. Additionally, a group of companies may opt to designate a single DPO.

Under Section 36 of the DPA 2018, the appointment of a DPO can be considered an appropriate and specific measure needed to protect the fundamental rights and freedoms of data subjects in certain cases.

Under Section 34 of the DPA 2018, the relevant Minister may establish regulations mandating controllers, processors, associations, or other bodies representing categories of controllers or processors to appoint a DPO. At the time of writing, no such regulations have been enacted in Ireland.

8.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

The penalty for failure to appoint a DPO, where one should have been appointed, is an administrative fine of up to EUR 10 million, or in the case of an undertaking, up to 2% of total worldwide annual turnover of the preceding financial year. Further corrective powers of the DPC may be invoked for breaches of the GDPR, e.g. the issuance of warnings and reprimands, orders to bring processing into compliance, orders to cease processing and the imposition of a ban on processing.

8.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

The designated DPO must not face dismissal or penalties from

a controller or processor for carrying out their duties. They are required to function autonomously and should report directly to the highest management level of the controller or processor.

8.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

A group of undertakings may appoint a single DPO, provided that they are easily accessible for each establishment.

8.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The DPO must be designated on the basis of professional qualities and in particular expert knowledge of data protection law and practices and the ability to fulfil tasks set out in the GDPR, these being: (i) informing and advising the controller or processor and the employees who carry out processing of their obligations under the GDPR and Irish data protection law; (ii) monitoring compliance with the GDPR and Irish data protection law; (iii) providing advice where requested in regard to the DPIA and monitoring its performance; (iv) cooperating with the DPC as supervisory authority; and (v) acting as the contact point for the DPC as supervisory authority on issues relating to processing.

8.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

The DPO is required to: (i) provide information and guidance to the controller or processor and the employees who carry out processing regarding their responsibilities under the GDPR and Irish data protection law; (ii) oversee adherence to the GDPR and Irish data protection law; (iii) offer advice upon request concerning DPIAs and supervise their implementation; (iv) collaborate with the DPC as the supervisory authority; and (v) act as the contact point for the DPC as supervisory authority on issues relating to processing.

8.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

The appointment of the designated DPO and their contact details must be notified to the DPC.

8.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

Where a controller appoints a DPO, it must publish the contact details of the DPO. This, however, does not necessarily mean that the DPO needs to be named in public-facing documents, as the contact details may be anonymised, e.g. an anonymised email address such as dpo@iclgbyrnewallaceshields.ie.

The transparency requirements of the GDPR require that the contact details of the DPO be furnished to data subjects at the time when personal data is collected from them.

9 Appointment of Processors

9.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes, the business is required to enter into a Data Processing Agreement with the processor on a mandatory basis, under Article 28 of the GDPR.

9.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The processor must be engaged through a binding written agreement, which sets out: (i) the subject matter for processing; (ii) the duration of processing; (iii) the nature and purpose of processing; (iv) the types of personal data and categories of data subjects; and (v) the obligations and rights of the controller.

This agreement should include terms that specify that the processor: (i) only acts on the documented instructions provided by the controller; (ii) enforces confidentiality obligations on all employees involved; (iii) ensures the security of the personal data it processes; (iv) adheres to the rules regarding the appointment of sub-processors; (v) implements measures to assist the controller in upholding the rights of data subjects; (vi) assists the controller in obtaining approval from the relevant data protection authority; (vii) either returns or securely destroys the personal data at the termination of the relationship (unless otherwise obligated by EU or Member State law); and (viii) furnishes the controller with all necessary information to demonstrate compliance with the GDPR.

10 Marketing

10.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

The ePrivacy Regulations, which transpose the ePrivacy Directive into Irish law, outline specific rules with regard to the use of marketing communications. Consent is required in respect of electronic direct marketing for new customers. Consent is not required in respect of electronic direct marketing for existing customers, where certain conditions are satisfied.

10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

Although the specific rules and requirements for consent in the ePrivacy Regulations generally apply to natural persons, in relation to direct marketing by telephone calls, there is no distinction in the ePrivacy Regulations between unsolicited telephone communications to individuals and those to companies and all other persons other than natural persons. The regulation of such direct marketing calls differs depending on whether they are made to landlines or to mobile phones.

Unsolicited direct marketing by fax and call by automated calling machine to companies and all persons other than natural persons are regulated on an opt-out basis, that is, they are permitted until the intended recipient notifies the sender that it does not consent.

10.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

Unsolicited marketing calls to landlines (but not mobiles) are permitted until the recipient opts out by informing the caller of their withdrawal of consent. Similarly, unsolicited fax marketing is permissible until the recipient opts out by informing the sender of their withdrawal of consent. Direct marketing via postal mail is not covered by the ePrivacy Regulations, but it remains subject to the requirements outlined in the GDPR and the DPA 2018.

10.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?

The ePrivacy Regulations apply to entities sending direct marketing communications to recipients in Ireland. Direct marketers operating from abroad, including those sending marketing from outside the EU, are subject to the laws of their respective jurisdictions. It is important to note that the GDPR has significant extraterritorial reach, providing rights and safeguards to data subjects within the EU, irrespective of where the processing occurs.

10.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

There is evidence of the DPC enforcing data protection and direct marketing laws across all sectors. Please also see our answers to questions 11.3 and 19.1.

10.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Data sets, such as the purchase or sale of marketing lists, are captured by the broad definitions of marketing and processing. Therefore, a controller must comply with all of the legal obligations applicable to the processing of personal data under the GDPR, including the fundamental principles as outlined above. A purchaser of a marketing list will need to verify the data's usability, i.e. ensuring its lawful collection and subsequent use. This would include reviewing the vendor's record of processing activities to ensure the vendor has complied with all legal requirements, such as obtaining valid consent and conducting a legitimate interest assessment.

10.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

The DPC lacks the authority to impose fines for violations of the ePrivacy Regulations but is empowered to instigate

prosecutions through the courts. However, it possesses other enforcement capabilities, such as conducting investigations based on complaints or its own initiative, issuing enforcement notices that mandate compliance with specific requirements, and the power to disclose the identities of parties responsible for breaches along with details of the infringements.

Breaches of the ePrivacy Regulations may lead to criminal prosecution through the Irish courts. Upon summary conviction, the sender of a marketing communication may face a fine not exceeding EUR 5,000 per offence, while on indictment, a fine not exceeding EUR 250,000 per offence. Notably, if a marketer sends 100 emails, each email can be held to be a separate offence.

11 Cookies

11.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

The ePrivacy Regulations prohibit the use of cookies or other tracking technologies that are not strictly necessary for the provision of the service, unless the user has given explicit consent to that use. The standard of consent is that set out in the GDPR. Consent for the placement of non-essential cookies is not valid if it was either bundled or obtained by way of pre-checked boxes that users must deselect. Controllers must ensure that opt-in consent is obtained for each purpose for which cookies are set and consent must be as easy to withdraw by the user as it was to provide in the first place.

11.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

Consent for cookies or other tracking technologies is required where the cookies or tracking technologies are non-essential. As a result, third-party, performance, targeting cookies, etc. will require opt-in consent that can be as easily withdrawn by the user as it was given.

11.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

There is evidence of the DPC enforcing the ePrivacy Regulations across all sectors. Unfortunately, the DPC yearly review for 2024 has not yet been published to provide specific figures; however, the DPC has imposed large fines in a number of high profile cases.

11.4 What are the maximum penalties for breaches of applicable cookie restrictions?

The DPC is not empowered by law to issue fines for breach of the ePrivacy Regulations and it is not an offence in Ireland to violate the legal requirements for cookies and other tracking technologies. However, the DPC does have other enforcement powers, e.g. complaint-based and/or own volition investigations of alleged contraventions, enforcement notices that oblige recipients to comply with specific requirements, and the power to publish the names of parties responsible for and details of ePrivacy breaches. Please also see our answer to question 10.7.

12 Restrictions on International Data Transfers

12.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Transfers of personal data from Ireland to non-EEA or “third” countries are governed by Chapter V of the GDPR. Such transfers are permitted either where there is a European Commission adequacy decision in place or, alternatively, where appropriate safeguards are implemented, such as standard contractual clauses (“SCCs”) or binding corporate rules (“BCRs”), under Article 46 of the GDPR. Derogations may also apply in limited circumstances under Article 49 of the GDPR, e.g. where a data subject explicitly consents.

In June 2021, the European Commission approved four separate modular sets of SCCs and the appropriate module to be used will depend on the data protection role of the data exporter and data importer. Where SCCs are used, they should comply with the EDPB recommendations (Recommendations 01/2020) on measures to support the implementation of the decision in C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems* (“*Schrems II*”). In particular, the exporter must carry out a transfer risk assessment and also identify and implement supplementary measures to ensure an “essentially equivalent” level of protection applies to the personal data throughout the transfer to the third country.

12.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

Absent an adequacy decision, businesses may make transfers to non-EEA jurisdictions by putting in place appropriate safeguards, such as SCCs or BCRs. Derogations may also apply in limited circumstances under Article 49 of the GDPR, e.g. where a data subject explicitly consents to the transfer.

Transfer of personal data to the US is also possible if the data importer has signed up to the EU–US Data Privacy Framework, which has been designed by the US Department of Commerce in consultation with the European Commission to provide businesses in the EU and the US with a mechanism to comply with data protection requirements when transferring personal data from the EU to participating US companies and government agencies.

12.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

Approval of the DPC *per se* is not required for transfers to non-EEA jurisdictions. However, BCRs require approval of the relevant supervisory authority. There are, at the time of writing, 21 such approved BCRs for which the DPC is the lead supervisory authority (“LSA”). SCCs are those adopted by the European Commission, with the Commission having approved four separate modular sets of SCCs in June 2021.

As noted above, transfers to non-EEA or “third” countries are permitted where there is a European Commission adequacy decision in place or alternatively where appropriate safeguards are implemented, such as SCCs or BCRs.

12.4 Do transfers of personal data to other jurisdictions require a transfer impact assessment? If conducting a transfer impact assessment is only mandatory in some circumstances, please identify those circumstances.

A Transfer Impact Assessment (“TIA”) is only required when transferring personal data to a third country outside the EEA that is not covered by a European Commission adequacy decision. Conducting a TIA is a legal obligation for all EU-based data exporters who intend to carry out a restricted transfer by relying on one of the transfer tools in Article 46 of the GDPR.

12.5 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?

Although the DPC has not issued any official guidance following *Schrems II*, it has noted on its website that *Schrems II* will have an impact on BCRs, in that, before making transfers within a corporate group from members within the EEA to members in third countries, and taking into account the specific circumstances of the transfer, an assessment must be carried out on the level of protection and possible need for supplementary measures or suspension of the transfer.

12.6 What guidance (if any) has/have the data protection authority(ies) issued in relation to the use of standard contractual/model clauses as a mechanism for international data transfers?

The EDPB has issued Recommendations 01/2020 on supplementary protections to be implemented where appropriate, in respect of transfers made under SCCs, in light of the *Schrems II* decision. These Recommendations are designed to assist data exporters with the task of assessing the laws of third countries and identifying appropriate measures to implement where the level of protection afforded to personal data is not essentially equivalent to that within the EEA. Such protections include technical measures (e.g. pseudonymising personal data or encrypting it while in transit), contractual measures (e.g. certification by a data importer that it has not created any “back doors” that could be used to access the personal data or contractual provision for a “warrant canary” method) and organisational measures (e.g. ensuring adequate internal policies that contain clear allocation of responsibilities for data transfers or regular publication of transparency reports).

13 Whistle-blower Hotlines

13.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

The Protected Disclosures Act 2014, as amended (the “2014 Act”), transcribes EU Directive 2019/1937 on the protection of

persons who report breaches of Union law (commonly known as “**whistleblowing**”). The 2014 Act sets out detailed requirements and obligations in relation to internal whistleblowing reporting channels for employers with over 50 employees. The 2014 Act details the types of wrongdoing to which it applies, the categories of persons who will be protected if they make a report of a wrongdoing, and the protections applying to the reporting person, including protection of identity and protection from penalisation. The 2014 Act also sets out the process for accepting, acknowledging and following up on reports of wrongdoing from reporting persons. Processing of such personal data will mainly be carried out in order to comply with the legal obligations set out in the 2014 Act.

The 2014 Act permits limitations on certain data protection rights and obligations provided for in Articles 12 to 22 and Article 34 of the GDPR, where necessary and proportionate. This is done to, among other objectives, prevent and address efforts to obstruct reporting or impede the follow-up on reports, or to uncover the identity of whistle-blowers.

Although the 2014 Act establishes minimum requirements, it does not restrict corporate whistleblowing processes from exceeding its provisions. Companies may accept reports on a broader range of issues and from a wider array of individuals, or may implement processes for employers with fewer than the specified number of employees. Processing of personal data in such cases should be conducted on a lawful basis as per Article 6 of the GDPR, which may include the legitimate interests of the employer.

13.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

According to the 2014 Act, employers are not compelled to receive and act upon anonymous reports; nonetheless, they retain the option to do so if they so choose. In the event that an anonymous report is accepted, it must be handled in a manner consistent with any other report made under the 2014 Act, to the fullest extent possible considering its anonymous nature. Employers have the discretion to stipulate in their relevant internal policy whether they will accept anonymous reports.

14 CCTV

14.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

Where a controller determines by way of a DPIA that the intended processing would result in a high risk to the data protection rights of individuals then, in the absence of mitigation measures, they must consult with the DPC. In addition, where the monitoring of publicly accessible areas (whether by CCTV or otherwise) is being undertaken on a large scale, the recitals to the GDPR state that a DPIA is required.

Beyond this, no specific prior registration/notification or prior approval is required for CCTV use.

The DPC has issued guidance on the use of CCTV, which includes a “CCTV Checklist”, the questions on which should be considered prior to installing a CCTV system. These questions include:

- (i) Do you have a clearly defined purpose for installing CCTV?
- (ii) What is the legal basis for your use of CCTV?
- (iii) Can you demonstrate that CCTV is necessary to achieve your goal?
- (iv) If your CCTV system is to be used for purposes other than security, are you able to demonstrate that those other uses are proportionate?

In addition to considering the CCTV Checklist, best practice recommends that a controller puts in place a CCTV policy that is compliant with DPC guidelines. Controllers should also ensure that data subjects are informed of their rights in respect of their personal data processed through the use of CCTV and that the CCTV policy is published on the controller’s website, so that members of the public visiting the controller’s premises are aware of the policy in advance. Prominent and visible signage should be displayed to make data subjects aware of the presence of CCTV.

14.2 Are there limits on the purposes for which CCTV data may be used?

Although the DPC guidance does not provide any limits on the purposes for which CCTV data may be used, it does advise that unless CCTV is used proportionately, it can give rise to legitimate concerns of unreasonable and unlawful intrusion into the data protection and privacy rights of individuals and monitoring or surveillance may be taking place. The DPC guidance further states that a controller must be able to justify the use of a CCTV system as both necessary to achieve their given purposes and proportionate in its impact upon those who will be recorded.

15 Employee Monitoring

15.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Employee monitoring is permitted by employers, provided that there is a lawful basis to do so. The type of monitoring permitted will depend on the nature and circumstances of the employment, and extent of monitoring being carried out. Employees must be informed that the monitoring is being carried out, and the purpose for which it is being carried out.

Any monitoring of employees must be proportionate to the purpose of the processing and the infringement on their right to privacy must be balanced with the objective the monitoring seeks to achieve.

15.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

While consent is one such lawful basis, it is seldom used in employment contexts, due to concerns regarding the imbalance of power between employers and employees, which could affect the validity of such consent. According to the EDPB Guidelines 05/2020 on consent under the GDPR, relying on employee consent for most data processing at work is discouraged.

Instead, employers typically rely on the lawful basis of legitimate interest to justify employee monitoring. However, this requires that the monitoring is proportionate, necessary to achieve the legitimate interest, and does not override the

interests or fundamental rights and freedoms of the employee. Notice of monitoring should be provided, usually through a data protection policy or other relevant employment policy, to ensure transparency and compliance with data protection regulations.

15.3 To what extent do works councils/trade unions/ employee representatives need to be notified or consulted?

There is no legal requirement to notify or consult with works councils or trade unions; however, such consultation may take place as part of best practice.

15.4 Are employers entitled to process information on an employee's attendance in office (e.g., to monitor compliance with any internal return-to-office policies)?

The DPC has not provided any specific guidance on employers monitoring their employees' attendance in the context of any internal return-to-office policies. However, the DPC has issued extensive guidance on the use of CCTV in the workplace and employee vehicle tracking. The DPC also recognises that employers have a legitimate interest in protecting their business, reputation, resources and equipment. To achieve this, they may decide to monitor their employees' use of the internet, email and telephone. The DPC warns, however, that any limitation of employees' right to privacy should be proportionate to the likely damage to the employer's legitimate interests. An acceptable-use policy should be adopted reflecting this balance and employees should be aware of the scope and purposes of the monitoring specified. In the absence of a clear acceptable-use policy, employees may be assumed to have a reasonable expectation of privacy in the workplace.

16 Data Security and Data Breach

16.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Yes. Both controllers and processors are obliged to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk arising from processing activities. Neither the GDPR, nor the DPA 2018, stipulate any specific security measures other than in Article 32, which mentions both pseudonymisation and encryption as examples. The GDPR lists certain considerations that should be taken into account, such as the costs of implementation and the nature, scope, context and purposes of processing. The DPC has issued Guidance for Controllers on Data Security in February 2020.

The ePrivacy Regulations impose certain security obligations on undertakings providing a publicly available electronic communications network or service. Security measures must at least ensure that the personal data can be accessed only by authorised personnel for legally authorised purposes, protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure, and ensure the implementation of a security policy with respect to the processing of personal data.

16.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

A controller is responsible for reporting a personal data breach without undue delay (and in any case within 72 hours of first becoming aware of the breach) to the relevant data protection authority, unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject(s). A controller must document any personal data breach.

The notification must include, at least, the following information: (i) the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; (ii) the name and contact details of the DPO or other contact point; (iii) the likely consequences of the personal data breach; and (iv) the measures taken or proposed to be taken by the controller to address the breach, including, where appropriate, measures to mitigate its possible adverse effects. A processor must also notify any data breach to their controller without undue delay.

16.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Controllers are obliged to notify affected data subjects of the personal data breach where the breach is "likely to result in a high risk to the rights and freedoms of the natural person". No such reporting obligation to the data subject arises where: (i) the controller has implemented technical and organisational measures that render the personal data unintelligible to third parties, e.g. encryption; (ii) the controller has taken subsequent measures to ensure that the high risk to the data subject's rights do not materialise; or (iii) it would involve disproportionate effort.

The notification must describe in clear and plain language the nature of the breach and at the least: (i) the name and contact details of the DPO or other contact point; (ii) the likely consequences of the personal data breach; and (iii) the measures taken or proposed to be taken by the controller to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where notification to the data subjects is deemed to involve disproportionate effort, the controller must attempt alternative methods to make the data subjects aware of the processing such as a media notification.

16.4 What are the maximum penalties for personal data security breaches?

Regulatory fines for breaches of data protection law can be up to the greater of EUR 20 million or 4% of global annual turnover of the relevant organisation for the preceding financial year, depending on the nature of the infringement. Other sanctions include a temporary or permanent ban on the processing of personal data, a reprimand or withdrawal of certification.

The DPC has various and wide powers, in addition to or as an alternative to a financial penalty, e.g. powers to issue a warning, impose a reprimand, issue various orders such as order a controller to comply with the data subject's request(s), to bring processing operations into compliance or to impose a ban on processing.

The DPA 2018 imposes a maximum fine of up to EUR 1 million on public authorities, or bodies that do not act as an undertaking within the meaning of the Irish Competition Act 2002.

The maximum criminal penalty for summary offences under the DPA 2018 is EUR 5,000 and/or 12 months' imprisonment. Indictable offences carry a maximum penalty of EUR 250,000 and/or five years' imprisonment.

The DPC does not have the power to impose regulatory fines pursuant to the ePrivacy Regulations. However, it has the power to prosecute offences under these regulations. A summary offence carries a maximum fine of EUR 5,000. Indictable offences carry a maximum fine of EUR 250,000, depending on the nature of the offence being prosecuted.

17 Enforcement and Sanctions

17.1 Describe the enforcement powers of the data protection authority(ies).

- (a) **Investigative powers:** The DPC possesses broad investigatory (and enforcement) powers, including: (i) search and seizure powers; (ii) powers to issue information and enforcement notices for which failure to comply is an offence; and (iii) the right to apply to the Irish High Court for the suspension or restriction of processing of data, where it is considered that there is an urgent need to act. The DPC also has the power to prosecute offences under the Act and the ePrivacy Regulations.
- (b) **Corrective powers:** The DPC possesses broad corrective powers including: (i) powers to issue warnings or reprimands for non-compliance; (ii) to order the controller to disclose a personal data breach to the data subject; (iii) to impose a permanent or temporary ban on processing; and (iv) to impose an administrative fine.
- (c) **Authorisation and advisory powers:** The DPC possesses broad authorisation and advisory powers, including: (i) advise controllers; (ii) issue opinions to the government or other institutions; (iii) authorise processing; (iv) issue opinions and draft codes of conduct; (v) accredit certification bodies; (vi) issue certifications; and (vii) adopt and authorise SCCs and approve BCRs.
- (d) **Imposition of administrative fines for infringements of specified legal provisions:** The DPC may impose regulatory fines for breaches of data protection law of up to EUR 20 million or 4% of global annual turnover of the relevant organisation for the preceding financial year, whichever is the greater, depending on the nature of the infringement.
- (e) **Non-compliance with a data protection authority:** Failure to comply with the DPC (or any supervisory authority under the GDPR) under Article 31 of the GDPR, may give rise to a fine under Article 83(4) of the GDPR of the higher of EUR 10 million or 2% of global annual turnover of the relevant organisation for the preceding financial year, whichever is the greater.

17.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

Section 134 of the DPA 2018 permits the DPC, where it identifies an urgent need to protect data subjects' rights and freedoms under a relevant act or statutory instrument, to make an application to the High Court (which may be *ex parte* under Section 134(4) of the DPA 2018) for an order to suspend, restrict or prohibit the processing of personal data.

17.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

The DPC has acquired a reputation as an active enforcement body by virtue of the GDPR's "one-stop-shop mechanism" ("OSS"), which allows organisations that are engaged in cross-border EU data processing to deal with a single LSA for their data protection compliance obligations.

While there was no record fine in 2024, the DPC remained active and was responsible for enforcing more than half of the €1.2 billion in European data fines in 2024.

These included the conclusion of investigations into LinkedIn and their use of personal data for the purposes of behavioural analysis and targeted advertising and also the investigation into a personal data breach by Meta affecting 29 million Facebook users worldwide and 3 million based within the EU/EEA. Final decisions in these matters resulted in a €310 million fine against LinkedIn and €251 million against Meta. The DPC also recently levied a fine of €530 million on TikTok for non-compliance with the requirements of the GDPR in respect of its transfers of personal data to China.

17.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

The OSS facilitates the regulation of entities established in the EU that engage in cross-border processing. It comes into effect when an entity conducts cross-border processing and has multiple establishments within the EU. The LSA for such an entity is the supervisory authority of the Member State where the entity's main establishment is located. The LSA assumes primary responsibility for overseeing the entity's processing activities and serves as the main point of contact for cross-border processing matters in most instances. The OSS operates within the framework of the GDPR's cooperation and consistency mechanism.

In 2023, the DPC received 156 valid cross border complaints, relating to companies for whom the DPC is the LSA. Unfortunately, the annual report for 2024 is not yet published to provide updated figures at this juncture.

The DPC serves as the lead LSA for numerous multinational companies across the EU that have their European headquarters situated in Ireland. Notably, the DPC has taken on high-profile inquiries and enforcement actions, including the LinkedIn and Meta decisions, in 2024. It is important to note that the rules governing the LSA and the OSS do not apply to processing carried out by public authorities or private bodies in the public interest.

18 E-discovery/Disclosure to Foreign Law Enforcement Agencies

18.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

In the first instance, a business will typically check if the request is legitimate. A business must be satisfied that any processing of personal data pursuant to a request from a foreign enforcement agency is compliant with the GDPR, there must be a lawful basis for processing pursuant to Article 6, and in the case of special-category data, one of the conditions in Article 9 must also be satisfied.

Where requests for disclosure have been made by foreign law enforcement agencies, this data may constitute personal data relating to criminal convictions and offences. If this is the case, the business must also ensure compliance with Article 10 of the GDPR, and section 55 of the DPA 2018.

If processing is conducted for purposes other than those for which the data was collected, it is lawful to the extent that it is necessary and proportionate for:

- preventing a threat to national security, defence or public security;
- preventing, detecting, investigating or prosecuting criminal offences; or
- providing or obtaining legal advice in the context of legal proceedings or establishing, exercising and defending legal rights.

Given the risk and time involved in this legal assessment, businesses often direct the requestor to the mutual legal assistance process outlined in the Criminal Justice (Mutual Assistance) Act 2008. The Minister for Justice serves as the Irish Central Authority for Mutual Assistance, responsible for coordinating correspondence between domestic and foreign authorities for both incoming and outgoing requests, as well as performing administrative functions related to coordinating requests.

18.2 What guidance has/have the data protection authority(ies) issued on disclosure of personal data to foreign law enforcement or governmental bodies?

The DPC has issued general guidance on the legal bases for processing personal data but has not issued formal guidance addressing disclosure to foreign law enforcement agencies at the time of writing.

19 Artificial Intelligence

19.1 Are there any limitations on automated decision-making involving the processing of personal data using artificial intelligence?

The laws in Ireland governing the use of AI are primarily, but not exclusively, governed by Regulation 2024/1689 on harmonised rules on Artificial Intelligence (the “AI Act”). AI machine-based systems are designed to operate with varying levels of autonomy and can generate automated outputs such as predictions, content, recommendations and decisions. The AI Act regulates AI systems and AI models from a human-centric perspective. It requires providers of AI systems that are categorised as “high risk” to adopt a “human oversight by design” approach in their development of the technology.

Additionally, commercial users of AI systems (defined as “deployers” in the AI Act) are obliged to assign individuals to oversee the operation of such systems and to be aware of automation bias. In addition to the human-centric philosophy underpinning the AI Act, it is recognised that development and use of AI systems and models are closely associated with the processing of personal data. Article 2(7) of the AI Act provides that the use of personal data will remain governed by the GDPR and, in the case of EU institutions, by the EU Data Protection Regulation. The AI Act expressly states that it does not seek to affect the application of the GDPR.

Where providers and deployers of AI systems process personal data as part of the design, development and/or use of an AI system or model, they will do so in their roles as the controllers and processors of the personal data they process. Recital 22 to the AI Act also clarifies that data subjects will continue to enjoy their rights under the GDPR where they relate to automated decision-making and profiling by an AI system. The AI Act does not prohibit automated decision-making by AI systems *per se*, whereas Article 22 of the GDPR states that data subjects have the right not to be subject to a solely automated decision that results in an outcome affecting them legally or otherwise having a significant similar effect. An example of such an automated decision may be a negative credit score determined by a software algorithm that consequently impairs an individual’s borrowing ability. Article 22 therefore requires controllers to implement suitable measures to safeguard an individual’s rights and freedoms and legitimate interests. This must include at least the right to obtain human intervention on the part of the controller and for the individual to express their point of view and to contest the decision.

Notwithstanding the AI Act’s provisions that data protection is still governed by the GDPR, there is a degree of tension between both pieces of legislation in the operation of automated technology. It remains to be seen, from further guidance, whether the human oversight obligation in the AI Act concerning a high-risk systems will be sufficient to mean that a decision affecting an individual will not be considered solely automated for the purposes of the GDPR.

19.2 What guidance (if any) has/have the data protection authority(ies) issued in relation to the processing of personal data in connection with artificial intelligence?

The DPC has published guidance on data protection considerations in the use of AI Large Language Models (“LLMs”). The guidance notes that Generative AI LLMs have grown in popularity for multiple use cases, including in workplace, home and education settings. The DPC guidance states the development and use of AI LLMs may involve personal data processing. Where organisations develop an AI model using personal data, they should consider whether they have a legal basis to do so, bearing in mind that publicly accessible personal data falls within the scope of the GDPR. Such organisations are required to account for the purposes that individuals have made their personal data publicly accessible to assess how it can be used. Providers of AI models must consider all risks associated with the product design, creation and prospective use. The consideration of these risks may require a DPIA, particularly where the technology or processing is new, where there is an intention to combine data sets in the training model or where the data concerns children or other vulnerable members of society. Additionally, if there are data sharing arrangements with other organisations to train the model, the organisations sharing the personal data are required to ensure that they have a legal

basis to do so and that the processing is fair and transparent. The DPC's guidance also covers obligations to ensure there is appropriate personal data governance, design, policy and decision-making controls in place in accordance with GDPR accountability requirements. Finally, providers of AI models should consider other legal obligations in relation to the use of data, such as copyright, safety and security requirements.

Where organisations use (as opposed to create /design) an AI model, they should be aware that they may be a controller of the personal data that the AI product uses. Organisations should consider the purpose and goal of the processing using AI technologies and whether there are alternative AI technologies that may be less risky or more appropriate. If it uses a third-party AI product, an organisation should obtain information from the relevant third party about the nature of personal data that the AI product uses, how both the provider and product use the personal data and whether the personal data is retained by the provider or reused in any way. The Guidance informs organisations that they should provide this information to affected data subjects in an understandable and accessible form, most likely in a privacy notice.

In August 2024, the DPC requested an opinion from the EDPB on the use of personal data for the development and deployment of AI models. The DPC's request focused on: (i) the circumstances where an AI model may be considered to be anonymous; (ii) how to demonstrate the appropriateness of legitimate interests as a basis to process personal data to develop or deploy an AI model; and (iii) the consequences of unlawful data processing in the development phase of an AI model on its subsequent operation. The EDPB's opinion on the use of personal data for the deployment and development of AI models was published in December 2024. In brief, the EDPB stated that whether an AI model is anonymous should be assessed on a case-by-case basis by a supervisory authority by reference to a non-prescriptive and non-exhaustive list of methods to demonstrate anonymity. The opinion sets out the three-part test that supervisory authorities should take account of to assess legitimate interests as an appropriate legal basis for the development and deployment of AI models. This includes a number of criteria to assist in assessing whether individuals may reasonably expect certain uses of their personal data, such as whether the data is publicly available, the nature of the relationship between the individual and the controller and the context in which the personal data was collected and whether individuals are aware that their personal data is online.

Where an AI model is developed using unlawfully processed personal data, the EDPB states that this could impact the lawfulness of the deployment of the AI model unless the model is anonymised. The EDPB's opinion has been welcomed by the DPC, which stated that it will enable proactive, effective and consistent regulation and assist the DPC in its engagement with companies developing AI models and with addressing AI-related complaints.

20 Trends and Developments

20.1 In your opinion, what enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.

The DPC is actively implementing its Regulatory Strategy for 2022–2027¹ to ensure accountability among data controllers and processors. This strategy involves prioritising the consistent enforcement of data protection law by sanctioning proportionately and judiciously, and taking a fair and balanced approach to complaint handling. In 2025, we can expect that

there will be an increased focus on the protection of children and other vulnerable groups, the prioritisation of prosecution, sanctions and fines, and publishing guidance for small and medium-sized enterprises.

As discussed in our answer to question 17.3, the DPC remained active, accounting for over 50% of all European data fines and concluding two large investigations resulting in fines of €310 million (LinkedIn) and €251 million (Meta), and the recent fine of €530 million (TikTok).

20.2 In your opinion, what “hot topics” are currently a focus for the data protection regulator?

The EU AI Act will introduce significant requirements on data usage, transparency and risk management in terms of AI systems. The DPC will be required to monitor the use of personal data in the training of AI systems and is empowered to impose penalties for non-compliance with data protection obligations. The DPC has issued guidance on the implementation and use of AI systems, particularly with regard to the use of personal data to train LLMs. This is a clear indication that the DPC will be closely monitoring the use of these systems going forward. Organisations that are deploying AI systems will be required to adhere to strict rules on the processing of personal data for the purposes of AI training.

On 11 April 2025, the DPC opened a formal investigation into X regarding its use of users' personal data to train its AI model. The investigation will focus on the legality and transparency of using public posts to train AI. This is a matter that will garner a great deal of attention given the EDPB's approval for Meta to utilise public posts on Instagram and Facebook to train its own AI model.

Meta has received regulatory approval in Europe to train its AI models using public posts from adult users across Facebook and Instagram. The EDPB gave Meta the green light after a months-long delay triggered by privacy complaints filed in 11 countries. The DPC previously stepped in in 2024, pausing Meta's AI rollout in the region. Meta has now begun to process publicly shared European content, ranging from memes to comment threads, to improve the cultural and linguistic understanding of its generative AI tools.

EU–US data transfers have been subject to a good deal of uncertainty with recent developments in the US administration. The EU–US Data Privacy Framework will continue to be monitored by the European Commission to ensure an adequate level of protection for data transfers remains in place. The recent TikTok fine by the DPC in respect of its transfers to the US is indicative of an increased regulatory focus in this area.

The two UK adequacy decisions in place governing personal data transfers between the EU and the UK have recently been extended and are due to expire on 27 December 2025. Should they fail to be extended or if further or new adequacy decisions are not granted, alternative satisfactory safeguards would need to be adopted for any data transfers to the UK.

Acknowledgment

The authors would like to thank Alan Grace for his invaluable contribution in the preparation of this chapter. Alan is an Associate in Byrne Wallace Shields LLP in the Privacy and Data Protection Team.

Endnote

¹ https://www.dataprotection.ie/sites/default/files/uploads/2021-12/DPC_Regulatory%20Strategy_2022-2027.pdf



Victor Timon is Head of the Technology Group at Byrne Wallace Shields LLP. He has nearly 40 years' experience in the technology industry, having worked both as an in-house Counsel in global technology companies and as a Partner in a number of law firms in Dublin and London. Victor's practice has evolved from more traditional IT projects (such as software licensing, equipment procurement, outsourcing, etc.) into cloud computing, e-commerce, digital communications, AI, block chain, NFTs, cyber security and social media. He is also an expert in intellectual property and data protection. He regularly speaks at in-people conferences and webinars and publishes articles on these topics. He has also authored the Ireland chapters of a number of international publications on AI, Digital Business and Cybersecurity.

Byrne Wallace Shields LLP
88 Harcourt Street, Dublin 2
Ireland

Tel: +353 1 691 5000
Email: vtimon@byrnewallaceshields.com
LinkedIn: www.linkedin.com/in/victortimontechprivacylawyer



Zelda Deasy is a Partner in the Byrne Wallace Shields LLP Corporate Department specialising in data protection and commercial contracts. She has over 20 years' experience in advising clients in the telecoms, technology, construction, energy, transport, life sciences, healthcare, financial services and FMCG sectors. Zelda's clients include companies at all stages of development from start-ups and entrepreneurs to SMEs and scaling companies to large domestic and multi-national organisations and public bodies. Zelda advises both private-sector organisations and public bodies on all data protection matters, including drafting, reviewing and negotiating data transfer/data sharing agreements, data processing agreements, online terms and conditions, privacy/cookies policies and data protection policies.

Byrne Wallace Shields LLP
88 Harcourt Street, Dublin 2
Ireland

Tel: +353 1 691 5000
Email: zdeasy@byrnewallaceshields.com
LinkedIn: www.linkedin.com/in/zeldadeasy



Seán O'Donnell is a Partner in Byrne Wallace Shields LLP and leads the firm's cross-departmental Privacy and Data Protection Team, overseeing and advising on all aspects of data protection law. Seán's background as a dispute resolution and regulatory lawyer is invaluable in engagements with the regulator, the Data Protection Commission. He advises clients on risk and mitigation of risk having regard to the Data Protection Regulatory Framework to include the e-Privacy Regulations. Seán also advises on the application of the Law Enforcement Directive. Seán has been instrumental in driving a cultural change amongst various clients to successfully embed compliance with GDPR within their organisations, having participated in several steering groups responsible for ensuring a GDPR-compliant framework is implemented and that such a framework can be adhered to in the practical undertaking of operations.

Byrne Wallace Shields LLP
88 Harcourt Street, Dublin 2
Ireland

Tel: +353 1 691 5000
Email: sodonnell@byrnewallaceshields.com
LinkedIn: www.linkedin.com/in/sean-o-donnell-206b2835



Jane O'Grady is a Partner at Byrne Wallace Shields LLP. Jane's practice area focuses on technology, data privacy and intellectual property. She has a particular specialism in advising on the use of emerging technologies, and in the development and commercialisation of digital goods and services including legal issues affecting the deployment of AI technology. Jane is the author of the Ireland chapter in the 2024 edition of *GLI – AI, Machine Learning & Big Data Laws and Regulations* published by GLG. She has also held a number of notable speaking engagements to industry and regulators on emerging legislation and regulation impacting technology. She is also the co-author of the Ireland chapter in the 2019 and 2020 editions of *ICLG – Trade Mark Laws and Regulations*.

Byrne Wallace Shields LLP
88 Harcourt Street, Dublin 2
Ireland

Tel: +353 1 691 5000
Email: jogrady@byrnewallaceshields.com
LinkedIn: www.linkedin.com/in/jane-o-grady-b74a092b

Byrne Wallace LLP and LK Shields Solicitors LLP merged on 1 January 2025 to form Byrne Wallace Shields LLP. The merger is one of the largest involving two Irish law firms and has created a firm with over 430 employees – including 220 solicitors. Byrne Wallace Shields LLP is a forward-thinking Irish law firm, focused on securing the best possible outcomes for our clients and is dedicated to the protection and promotion of our clients' interests through the provision of expert legal services. This expertise is borne out of close to half a century of delivering high professional standards and developing some of the most talented lawyers in Ireland. In recognition of the firm's commitment to delivering an excellent service to our clients and legal expertise, Byrne

Wallace Shields LLP has been awarded several national and international awards over the years.

www.byrnewallaceshields.com



Isle of Man

DQ Advocates Limited



Caitlin
Gelder



Kathryn
Sharman



Sinead
O'Connor

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The principal data protection legislation is the Data Protection Act 2018, which is supplemented by the GDPR and LED Implementing Regulations 2018 (the “**Regulations**”), as well as the Data Protection (Application of GDPR) Order 2018 and the Data Protection (Application of the LED) Order 2018 (together, the “**Orders**”).

1.2 Is there any other general legislation that impacts data protection?

The Regulations anticipate that the Information Commissioner (the “**ICO**”) will issue a data sharing Code, a direct marketing Code and any other Codes required to be issued by the Council of Ministers. These have generally not been issued at the time of writing, although a number of the Codes of Practice previously issued by the ICO remain of relevance. The ICO has also issued a number of “Closer Look” guides to support compliance with the Regulations and the Orders.

1.3 Is there any sector-specific legislation that impacts data protection?

The 2016 Code of Practice on Access to Government Information imposes additional data compliance obligations on government departments and public sector workers.

1.4 What authority(ies) are responsible for data protection?

The ICO is the independent supervisory body for data protection. The ICO has also been the supervisory body for the current Unsolicited Communications Regulations (the “**UCR**”) since 2005. In addition, the ICO holds certain responsibilities in respect of the Isle of Man Government’s Code of Practice on Access to Government Information and also holds an adjudication role in respect of the Freedom of Information Act 2015.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **“Personal Data”**
The Regulations currently define personal data as meaning “any information relating to an identified or identifiable living individual”. “Identifiable living individual” is further defined to mean “a living individual who can be identified, directly or indirectly, in particular by reference to: (a) an identifier such as a name, an identification number, location data or an online identifier; or (b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual”.
- **“Processing”**
“Processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- **“Controller”**
“Controller” means the natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data. This definition is, however, qualified by the Regulations so that where data is processed only: (a) for purposes for which it is required by an enactment to be processed; and (b) by means of which an enactment is required to be used for such processing, the controller is the person on whom the obligation to process the data is imposed by the enactment or any one of the enactments (if there are more than one). The definition is also subject to the provisions on the application of the Regulations to the Crown and to Tynwald (the Isle of Man Parliament).
- **“Processor”**
“Processor” means a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller.
- **“Data Subject”**
“Data Subject” means the identified or identifiable living individual to whom personal data relates.

- **“Sensitive Personal Data”/“Special Categories of Personal Data”**
“Sensitive Personal Data” is personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union memberships, data concerning health or sex life and sexual orientation, genetic data or biometric data. This is now referred to as “Special Category Data” for the purposes of the Regulations and the Orders.
- **“Data Breach”**
“Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
- **Other key definitions:**
 - **“Biometric Data”** means personal data resulting from specific technical processing, relating to the physical, physiological or behavioural characteristics of an individual, that allow or confirm the unique identification of that individual, such as facial images or dactyloscopic data.
 - **“Data Concerning Health”** means personal data relating to the physical or mental health of an individual, including the provision of healthcare services that reveal information about his or her health status.
 - **“Genetic Data”** means personal data relating to the inherited or acquired genetic characteristics of an individual that give unique information about the physiology or the health of that individual and which result, in particular, from an analysis of a biological sample from the individual in question.

3 Territorial and Material Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The Regulations apply to the following:

- A data controller established in the Island where the personal data is processed in the context of the activities of that establishment.
- A data processor processing personal data where the data processor is established in the Island and the personal data is processed in the context of the activities of that establishment.
- A data controller or data processor processing personal data where the data controller or data processor is not established in the Island but uses equipment in the Island for processing the personal data other than for the purposes of transit through the Island.
- A data controller established outside the Island where the personal data being processed relate to an individual who is in the Island when the processing takes place and the purpose of the processing is to offer goods or services to individuals in the Island, whether or not for payment or to monitor individuals’ behaviour in the Island.
- A data processor processing personal data for a data controller outside the Island or a data processor outside the Island where the personal data being processed relate to an individual who is in the Island when the processing takes place and the purpose of the processing is to offer goods or services to individuals in the Island,

whether or not for payment or to monitor individuals’ behaviour in the Island.

3.2 Do the data protection laws in your jurisdiction carve out certain processing activities from their material scope?

Within the Isle of Man, processing by a natural person in the course of a purely personal or household activity is not captured under the Data Protection legislation.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
Personal data must be processed lawfully, fairly and in a transparent manner. Controllers must provide certain minimum information to data subjects regarding the collection and further processing of their personal data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
- **Lawful basis for processing**
Processing of personal data is lawful only if, and to the extent that, it is permitted under Isle of Man data protection law. The law provides an exhaustive list of legal bases on which personal data may be processed, of which the following are the most relevant for businesses: (i) prior, freely given, specific, informed and unambiguous consent of the data subject; (ii) contractual necessity (i.e., the processing is necessary for the performance of a contract to which the data subject is a party, or for the purposes of pre-contractual measures taken at the data subject’s request); (iii) compliance with legal obligations (i.e., the controller has a legal obligation to perform the relevant processing); or (iv) legitimate interests (i.e., the processing is necessary for the purposes of legitimate interests pursued by the controller, except where the controller’s interests are overridden by the interests, fundamental rights or freedoms of the affected data subjects).
- **Purpose limitation**
Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes. If a controller wishes to use the relevant personal data in a manner that is incompatible with the purposes for which they were initially collected, it must: (i) inform the data subject of such new processing; and (ii) be able to rely on a lawful basis as set out above.
- **Data minimisation**
Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed. A business should only process the personal data that it actually needs to process in order to achieve its processing purposes.
- **Proportionality**
Personal data must be accurate and, where necessary, kept up to date. A business must take every reasonable step to ensure that personal data that are inaccurate are either erased or rectified without delay.

- **Retention**
Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- **Accuracy**
Reasonable steps must be taken to ensure that the personal data held is not incorrect or misleading. If it is found that personal data is incorrect or misleading, then reasonable steps must be taken to correct or delete it as soon as possible.
- **Data security**
Personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- **Accountability**
The controller is responsible for, and must be able to demonstrate, compliance with the data protection principles set out above. This includes compliance with the rights of data subjects.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to (copies of) data/information about processing**
A data subject has the right to obtain from a controller the following information in respect of the data subject's personal data: (i) confirmation of whether, and where, the controller is processing the data subject's personal data; (ii) information about the purposes of the processing; (iii) information about the categories of data being processed; (iv) information about the categories of recipients with whom the data may be shared; (v) information about the period for which the data will be stored (or the criteria used to determine that period); (vi) information about the existence of the rights to erasure, to rectification, to restriction of processing and to object to the processing; (vii) information about the existence of the right to complain to the relevant data protection authority; (viii) where the data were not collected from the data subject, information as to the source of the data; and (ix) information about the existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on the data subject. Additionally, the data subject may request a copy of the personal data being processed.
- **Right to rectification of errors**
Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data subjects have the right to rectification of inaccurate personal data.
- **Right to deletion/right to be forgotten**
Data subjects have the right to erasure of their personal data (the "right to be forgotten") if: (i) the data are no longer needed for their original purpose (and no new lawful purpose exists); (ii) the lawful basis for the processing is the data subject's consent, the data subject withdraws that consent, and no other lawful ground exists; (iii) the data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing; (iv) the data have been processed

unlawfully; or (v) erasure is necessary for compliance with data protection law.

- **Right to object to processing**
Data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data where the basis for that processing is either public interest or legitimate interest of the controller. The controller must cease such processing unless it demonstrates compelling legitimate grounds for the processing that override the interest, rights and freedoms of the relevant data subject or requires the data in order to establish, exercise or defend legal rights.
- **Right to restrict processing**
Data subjects have the right to restrict the processing of personal data, which means that the data may only be held by the controller, and may only be used for limited purposes if: (i) the accuracy of the data is contested (and only for as long as it takes to verify that accuracy); (ii) the processing is unlawful and the data subject requests restriction (as opposed to exercising the right to erasure); (iii) the controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights; or (iv) verification of overriding grounds is pending, in the context of an erasure request.
- **Right to data portability**
Data subjects have a right to receive a copy of their personal data in a commonly used machine-readable format, and to transfer their personal data from one controller to another or have the data transferred directly between controllers.
- **Right to withdraw consent**
A data subject has the right to withdraw their consent at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject must be informed of the right to withdraw consent. It must be as easy to withdraw consent as to give it.
- **Right to object to marketing**
Data subjects have the right to object to the processing of personal data for the purpose of direct marketing, including profiling.
- **Right protecting against solely automated decision-making and profiling**
Data subjects have the right not to be subject to a decision that is based solely on automated processing (including profiling), which produces legal effects concerning them or significantly affecting them.
- **Right to complain to the relevant data protection authority(ies)**
Data subjects have the right to lodge complaints concerning the processing of their personal data with the ICO, if the data subjects live in the Isle of Man or the alleged infringement occurred in the Isle of Man.

5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

Data subjects can make a complaint to the Isle of Man ICO. The ICO deals with complaints on the following:

- data protection legislation;
- the UCR (Electronic Direct Marketing);
- the Freedom of Information Act; and
- the Code of Practice on Access to Government Information.

The specific right for a data subject to mandate a not-for-profit organisation to seek a remedy on their behalf or to seek collective redress is not included in the Isle of Man’s data protection framework.

6 Children’s Personal Data

6.1 What additional obligations apply to the processing of children’s personal data?

The Data Protection (Application of GDPR) Order 2018 (the “**applied GDPR**”) makes specific reference to children and the processing of their data.

Specific protection should be applied to the use of personal data of children for the purposes of marketing or creating personality or user profiles, as well as to the collection of personal data with regard to children when using services offered directly to a child.

Data controllers must be aware if they process children’s data and ensure there are adequate safeguards and procedures in place as the following provisions apply to, or restrict, processing:

- **Article 6(1)(f)** – Legitimate interest ground for processing. Processing the personal data of children represents an enhanced risk.
- **Article 8** – Conditions applicable to a child’s consent in relation to information society services. Consent cannot be given by a child below the age of 13.
- **Article 12** – Fair processing information. Fair processing information “addressed to a child, should be in such a clear and plain language that the child can easily understand”.
- **Article 17** – Right to erasure. “[Where] the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child.”
- **Article 22** – Automated decisions, including profiling, are not permitted.

7 Registration Formalities and Prior Approval

7.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

Personal data must not be processed unless an entry in respect of the data controller is included in the register maintained by the ICO, subject to certain exemptions. The registration requirement also extends to data processors.

7.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

Registration is limited to some basic information in relation to the controller or processor, including the nature of its business and the details of the Data Protection Officer (“**DPO**”) or other appropriate contact.

In April 2025, the ICO launched a new online registration portal. This system will enable organisations to register, renew and amend their details (including email addresses and DPO details) through a self-service portal.

7.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

Registration is required on a “per data controller” or “per data processor” basis.

7.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

The Regulations require every controller and processor to which the applied GDPR applies, to register subject to certain exemptions, which are set out in Schedule 7 to the Regulations. Section 3 above sets out the scope of the Regulations in terms of the entities to which they apply.

7.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

Registration is limited to some basic information in relation to the controller or processor, including the nature of its business and the details of the DPO or other appropriate contact.

7.6 What are the sanctions for failure to register/notify where required?

Controllers and processors commit an offence if they process data without a registration when there is no applicable exemption, and when they fail to notify the ICO of changes to their registration information. These offences carry fines of up to £10,000 and directors may also be personally liable for offences.

7.7 What is the fee per registration/notification (if applicable)?

Fees are prescribed by the Treasury in the Data Protection (Fees) Regulations 2018. The fees are currently set at £70, although the ICO notes that the Council of Ministers may decide to amend that in the future. Exemptions from fees are available for relevant bodies where processing is limited to certain activities.

7.8 How frequently must registrations/notifications be renewed (if applicable)?

Registration must be renewed annually.

7.9 Is any prior approval required from the data protection regulator?

Prior approval in advance of registration is not required.

7.10 Can the registration/notification be completed online?

The registration can be completed online via the ICO's website.

The new online personal data breach reporting system and a self-service portal for registration and renewal allow organisations to submit directly to the ICO online without the need to download, complete and email the manual form.

7.11 Is there a publicly available list of completed registrations/notifications?

There is a publicly available list of completed registrations, which is available on the ICO's website.

7.12 How long does a typical registration/notification process take?

As registration can be completed online, it is an almost instant process, with the ICO then issuing an acknowledgment and payment details shortly thereafter.

8 Appointment of a Data Protection Officer

8.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The appointment of a DPO for controllers or processors is only mandatory in some circumstances, including where there is: (i) large-scale regular and systematic monitoring of individuals; or (ii) large-scale processing of special-category personal data. Where a business designates a DPO voluntarily, the requirements of the GDPR apply as though the appointment were mandatory.

8.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

In the circumstances where appointment of a DPO is mandatory, failure to comply may result in a penalty.

8.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

The appointed DPO should not be dismissed or penalised for performing their tasks and should report directly to the highest management level of the controller or processor.

8.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

A single DPO is permitted by a group of undertakings, provided that the DPO is easily accessible from each establishment.

8.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The DPO should be appointed on the basis of professional qualities and should have an expert knowledge of data protection law and practices. While this is not strictly defined, it is clear that the level of expertise required will depend on the circumstances. For example, the involvement of large volumes of sensitive personal data will require a higher level of knowledge.

8.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

A DPO should be involved in all issues that relate to the protection of personal data. The applied GDPR outlines the minimum tasks required by the DPO as including: (i) informing the controller, processor and their relevant employees who process data of their obligations under the law; (ii) monitoring compliance with data protection legislation and internal policies in relation to the processing of personal data including internal audits; (iii) advising on data protection impact assessments and the training of staff; and (iv) co-operating with the data protection authority and acting as the authority's primary contact point for issues related to data processing.

8.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

Yes, the controller or processor must notify the data protection authority of the contact details of the designated DPO.

8.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

The DPO does not necessarily need to be named in the public-facing privacy notice. However, the contact details of the DPO must be notified to the data subject when personal data relating to that data subject are collated.

9 Appointment of Processors

9.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes. The business that appoints a processor to process personal data on its behalf is required to enter into an agreement with the processor that sets out the subject matter for processing, the duration of processing, the nature and purpose of processing and the obligations and rights of the controller (i.e., the business).

It is essential that the processor appointed by the business complies with data protection requirements.

9.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The processor must be appointed under a binding agreement

in writing. The contractual terms must stipulate that the processor: (i) only acts on the documented instructions of the controller; (ii) imposes confidentiality obligations on all employees; (iii) ensures the security of personal data that it processes; (iv) abides by the rules regarding the appointment of sub-processors; (v) implements measures to assist the controller with guaranteeing the rights of data subjects; (vi) assists the controller in obtaining approval from the DPO; (vii) either returns or destroys the personal data at the end of the relationship; and (viii) provides the controller with all the information necessary to demonstrate compliance with the data protection requirements.

10 Marketing

10.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

The following provisions apply:

- Direct marketing activities must generally comply with the Regulations, and the applied GDPR and direct marketing communicated by electronic messages (including email, SMS and picture messaging) must comply with the UCR.
- Persons marketing by way of electronic mail (email, SMS or picture messaging) must obtain consent of the individual prior to transmission, or instigation of transmission, unless the conditions of a “soft opt-in” are met. The conditions of a soft opt-in are that: (i) the person marketing has obtained the relevant individual’s details in the course of selling or negotiating a sale of products or services offered by such person; (ii) the direct marketing only markets the same person’s similar products and services; (iii) the individual was given the opportunity to opt-out of marketing when their details were first collected but did not opt-out at that point; and (iv) the individual is given the opportunity to opt-out on each subsequent marketing communication.
- All consent requirements under the UCR can currently be validly obtained by either opt-in or opt-out consent.

The Regulations provide that the ICO will issue a direct marketing Code to contain practical guidance in relation to the carrying out of direct marketing in accordance with the requirements of the data protection legislation. This Code has not yet been made available.

10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

The restrictions that must be adhered to are applicable in both the business-to-consumer and business-to-business contexts, provided that the marketing is targeted at an individual. There are no separate regulations.

10.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

The following provisions apply:

- Direct marketing activities must generally comply with the Regulations and the applied GDPR, and direct marketing communicated by telephone calls or faxes must comply with the UCR.
- Direct marketing by post is not subject to specific regulation, but any processing of personal data for the purpose of direct marketing must be done in compliance with the principles of the Regulations and the applied GDPR.
- Persons marketing by way of live telephone calls may not make unsolicited calls if either: (i) the individual or corporation contacted has previously notified the person marketing that such calls should not be made to such individual’s or corporation’s telephone number; or (ii) the telephone number is listed on the register provided by the UK Telephone Preference Service (to whom the responsibility of maintaining the Isle of Man register has been delegated).
- Automated telephone marketing calls may only be made with the consent of the individual or corporation to whom such calls are directed.

The Regulations provide that the ICO will issue a direct marketing Code to contain practical guidance in relation to the carrying out of direct marketing in accordance with the requirements of the data protection legislation. This Code has not yet been made available.

10.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?

The ICO has a range of powers under the Regulations and the applied GDPR where breaches of marketing restrictions were due to data protection issues.

10.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

The ICO has a range of powers under the Regulations and the applied GDPR where breaches of marketing restrictions were due to data protection issues.

10.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

There is no legal restriction to prevent the purchase of marketing lists from third parties. A data controller would, however, have to give serious consideration to the origin of the list and the data subject’s awareness that their data has been sold in this way in order to ensure compliance with the data protection requirements.

10.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

There are no specific penalties set out in the current law. A person suffering damage by reason of contravention of the law is entitled to bring proceedings for financial compensation against the person contravening the law.

11 Cookies

11.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

The UCR implemented Article 13 of the European Privacy and Electronic Communications Directive (2002/58/EC) (the “**Privacy Directive**”). The UCR have not yet been amended to incorporate the changes made to the Privacy Directive in May 2011 regarding cookies. As a result, the requirements of the Privacy Directive are regarded as “best practice” only on the Isle of Man, and implementation of the guidance relating to cookies remains voluntary.

11.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

As above, there is no specific legislation or binding guidance regarding cookies on the Isle of Man.

11.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

There is no evidence that the ICO has taken any enforcement action in relation to cookies.

11.4 What are the maximum penalties for breaches of applicable cookie restrictions?

There are no relevant penalties.

12 Restrictions on International Data Transfers

12.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Under the Regulations and applied GDPR, data transfers to a third country can only take place if the transfer is to an “Adequate Jurisdiction” (as specified by the EU Commission) or approval has been obtained from the ICO in respect of any measures that the data controller is proposing to take in accordance with the applied GDPR. A third country is defined as a State, territory or jurisdiction other than the Isle of Man and which is not a Member State of the EU. The Isle of Man Parliament has approved the Data Protection (Withdrawal from the EU) (UK and Gibraltar) Regulations 2019, which enable data transfers to both territories to continue without additional safeguards post-Brexit.

12.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

Subject to approval from the ICO, when transferring personal data to a third country, businesses must ensure that there are

appropriate safeguards on the data transfer, as prescribed by the applied GDPR.

The applied GDPR offers a number of ways to ensure compliance for international data transfers, of which one is consent of the relevant data subject. Other common options are the use of Standard Contractual Clauses (“**SCCs**”) or Binding Corporate Rules (“**BCRs**”).

Businesses can adopt the SCCs drafted by the EU Commission – these are available for transfers between controllers, and transfers between a controller (as exporter) and a processor (as importer). International data transfers may also take place on the basis of contracts agreed between the data exporter and data importer, provided that they conform to the protections outlined in the applied GDPR and have prior approval by the relevant data protection authority.

International data transfers within a group of businesses can be safeguarded by the implementation of BCRs. The BCRs will always need approval from the relevant data protection authority. Most importantly, the BCRs will need to include a mechanism to ensure they are legally binding and enforced by every member in the group of businesses. Among other things, the BCRs must set out the group structure of the businesses, the proposed data transfers and their purpose, the rights of data subjects, the mechanisms that will be implemented to ensure compliance with the GDPR, and the relevant complaints procedures.

12.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

Under the applied GDPR, the ICO must approve any transfer of personal data to a third country that is not subject to an adequacy decision or where additional safeguards cannot be put in place.

12.4 Do transfers of personal data to other jurisdictions require a transfer impact assessment? If conducting a transfer impact assessment is only mandatory in some circumstances, please identify those circumstances.

A Transfer Impact Assessment (“**TIA**”) is a legal requirement when an EU-based data exporter intends to process a restricted transfer under Article 46 of the GDPR. A TIA is not required where the restricted transfer is to a country covered by the EU adequacy decision or an Article 49 exemption exists.

12.5 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?

Following the *Schrems II* case in 2020, the UK adopted two sets of SCCs, one to be used between controllers and processors within the EEA and the other for transfer of any personal data outside of the EEA. The new SCCs deem that an organisation must undertake a transfer risk assessment before they transfer data under Article 46.

12.6 What guidance (if any) has/have the data protection authority(ies) issued in relation to the use of standard contractual/model clauses as a mechanism for international data transfers?

The Isle of Man ICO has not published any independent advice on the use of standard contractual/model clauses in regard to international data transfers. The Isle of Man ICO website advises that there are clauses that can be used and points users towards the guidance issued by the European Commission.

13 Whistle-blower Hotlines

13.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

There is no reference to whistleblowing within the data protection law or regulations. Normal standards of data protection would be expected to apply to any data processed as a result of operating such a hotline.

13.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

There is no reference to whistleblowing within the data protection law or regulations and so there are no restrictions around anonymous reporting. Generally, regulatory and government guidance on whistleblowing encourages the reporter to disclose their name to assist in appropriate action being taken.

14 CCTV

14.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

Prior approval is not required from the ICO to use CCTV. A separate notification is also not required. The ICO's guidance recommends the use of clear and visible signage, which includes who to contact about the operation of the CCTV system.

14.2 Are there limits on the purposes for which CCTV data may be used?

The ICO's guidance states that there must be a lawful reason for considering the use of CCTV that cannot be met in another way. The ICO also suggests that the appropriateness for use of CCTV should be kept under review. Cameras should not be installed in private areas unless there are exceptional circumstances.

15 Employee Monitoring

15.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Employee monitoring is permitted, provided that compliance with the data protection legislation is achieved. Monitoring must be proportionate to the intended aim, not adversely impact the privacy of the individuals, and be justified by its benefit to the employer. It would generally be viewed as unfair to tell employees that monitoring is being undertaken for one purpose and then use the information obtained for another purpose.

15.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Employers are required, on an ongoing basis, to make employees aware of any monitoring that is undertaken and the reasons for it, except in the exceptional limited circumstances where covert monitoring is necessary. Consent would only be required where an employer needed to rely on it as a legitimising condition for the processing of the personal data in accordance with the data protection legislation. Employers typically provide notice through a range of measures such as inclusion in the staff handbook, notices in the workplace and regular reminders through formal and informal communications. Employers typically obtain consent through clear and specific fair-processing notices signed by the employees.

15.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

There is no requirement for such representatives to be notified or consulted.

15.4 Are employers entitled to process information on an employee's attendance in office (e.g., to monitor compliance with any internal return-to-office policies)?

Employees' attendance can be monitored so long as it is done in a way that is compliant with Data Protection Law. In order to process and collect the data from employees, a lawful basis for processing must be identified. In addition, the Privacy Notice for employees should be transparent as to the data collected, its purpose and the legal basis for processing.

16 Data Security and Data Breach

16.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Yes. Personal data must be processed in a way that ensures security and safeguards against unauthorised or unlawful processing, accidental loss, destruction and damage of the data.

Both controllers and processors must ensure they have appropriate technical and organisational measures to meet the requirements of the data protection legislation. Depending on the security risk, this may include the encryption of personal

data, the ability to ensure the ongoing confidentiality, integrity and resilience of processing systems, an ability to restore access to data following a technical or physical incident, and a process for regularly testing and evaluating the technical and organisational measures for ensuring the security of processing.

16.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

The controller is responsible for reporting a personal data breach without undue delay (and in any case within 72 hours of first becoming aware of the breach) to the relevant data protection authority, unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject(s). A processor must notify any data breach to the controller without undue delay.

The notification must include the nature of the personal data breach, including the categories and number of data subjects concerned, the name and contact details of the DPO or relevant point of contact, the likely consequences of the breach and the measures taken to address the breach, including attempts to mitigate possible adverse effects.

16.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Controllers have a legal requirement to communicate the breach to the data subject, without undue delay, if the breach is likely to result in a high risk to the rights and freedoms of the data subject.

The notification must include the name and contact details of the DPO (or point of contact), the likely consequences of the breach and any measures taken to remedy or mitigate the breach.

The controller may be exempt from notifying the data subject if the risk of harm is remote (e.g., because the affected data is encrypted), the controller has taken measures to minimise the risk of harm (e.g., suspending affected accounts) or the notification requires a disproportionate effort (e.g., a public notice of the breach).

16.4 What are the maximum penalties for personal data security breaches?

There is a maximum discretionary penalty of up to £1 million for breaches that are other than those prescribed in the GDPR.

17 Enforcement and Sanctions

17.1 Describe the enforcement powers of the data protection authority(ies).

- (a) **Investigative powers:**
 - The ICO has powers of entry and inspection.

- Information Notice – requires a controller or processor to provide the ICO with the information that he reasonably requires.

- Through a warrant, the ICO can access all personal data, information, premises and equipment as necessary.

- (b) **Corrective powers:**

- Enforcement Notice – requires the recipient to take the steps specified in the Notice or refrain from taking the steps specified in the Notice.

- Assessment Notice – requires a controller or processor to permit the ICO to carry out an assessment of compliance with the data protection requirements.

- (c) **Authorisation and advisory powers:** The Regulations provide the ICO with the power to issue various Codes of Practice.

- (d) **Imposition of administrative fines for infringements of specified legal provisions:** The ICO can issue a penalty in relation to the infringement of a provision of the applied GDPR. The maximum amount for this penalty is £1 million.

- (e) **Non-compliance with a data protection authority:** Failure to comply with an Information, Enforcement, Assessment or Penalty Notice may be certified to the High Court, which will treat the matter as contempt of court.

17.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The Regulations entitle the ICO to impose a temporary or definitive limitation, including a ban on processing.

17.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

Enforcement to date has been limited to Enforcement Notices and Formal Undertakings against Isle of Man data controllers.

17.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

Enforcement to date has included Penalty Notices, Enforcement Notices and Formal Undertakings against Isle of Man data controllers.

18 E-discovery/Disclosure to Foreign Law Enforcement Agencies

18.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

The duty of confidentiality and compliance with the data protection principles would be uppermost in the minds of companies responding to such requests. Traditionally, the obligation to exchange information, such as under automatic exchange of information regimes, would be covered in an organisation's terms and conditions. For data protection

reasons, though, exchange of information is often limited to Isle of Man statutory or public authorities, rather than data being released to foreign authorities. Isle of Man companies are very mindful of requests from foreign law enforcement agencies and would be keen to ensure that these have come through the appropriate channels in advance of replying to them.

18.2 What guidance has/have the data protection authority(ies) issued on disclosure of personal data to foreign law enforcement or governmental bodies?

The Isle of Man ICO has not issued any specific advice in regard to the disclosure of personal data to foreign law enforcement or government bodies.

Isle of Man Data Protection Law allows for the sharing of personal information with law enforcement and governmental bodies if it is proportionate and necessary. Transfer to a third country is permitted if the transfer is covered by an adequacy decision.

Where the adequacy regulations are not in place, the transfer may still be made where appropriate safeguards exist to determine that the rights of an individual are enforceable and legal remedy is available following the transfer.

19 Artificial Intelligence

19.1 Are there any limitations on automated decision-making involving the processing of personal data using artificial intelligence?

Under Article 22 of the GDPR, individuals have the right not to be subject to decisions based solely on automated processing, including profiling, that produce legal effects concerning them or significantly affect them. Such decisions are prohibited unless they are:

- necessary for entering into, or the performance of, a contract between the data subject and a data controller;
- required or authorised by domestic law, which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
- based on the data subject's explicit consent.

Individuals must be informed about the existence of automated decision-making processes. Additionally, individuals have the right to obtain human intervention, express their point of view and contest the decision.

Moreover, all processing of personal data, including by AI systems, must comply with the fundamental data protection principles, such as lawfulness, fairness, transparency and accountability.

19.2 What guidance (if any) has/have the data protection authority(ies) issued in relation to the processing of personal data in connection with artificial intelligence?

The Isle of Man ICO has not yet issued specific guidance exclusively addressing the processing of personal data in connection with AI. However, the Commissioner has provided comprehensive guidance on data protection principles and accountability under the GDPR, which are applicable to AI systems.

20 Trends and Developments

20.1 In your opinion, what enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.

Since April 2024, the Isle of Man ICO has issued three Enforcement Notices, demonstrating an active stance on data protection compliance.

Two Urgent Enforcement Notices were issued to secondary schools requiring them to cease the use of surveillance systems installed "inside" student toilet/restroom facilities. These notices were issued on the grounds that the schools had not carried out appropriate data protection risk assessments, and the processing of personal data in these environments was deemed disproportionate and intrusive.

A third Enforcement Notice was issued to a healthcare organisation following a complaint regarding the handling of a Subject Access Request (SAR) by a former employee. The Commissioner found that the organisation had conducted excessive and unnecessary searches, failing to respond to the SAR in a targeted and proportionate manner.

20.2 In your opinion, what "hot topics" are currently a focus for the data protection regulator?

One notable development is the March 2024 guidance on the use of domestic surveillance equipment, such as CCTV and doorbell cameras by individuals. While personal use within a private boundary may not require registration, individuals must still comply with core data protection principles, including purpose limitation and data minimisation.

The Commissioner is also actively promoting transparency and accountability through improved processes, such as the introduction of a new online personal data breach reporting system and a self-service portal for registration and renewal. These changes are intended to streamline compliance for organisations operating under the Isle of Man's data protection laws.



Caitlin Gelder is an advisor in DQ's Regulatory & Compliance Services Team. Caitlin holds an ICA Governance, Risk and Compliance Diploma.

DQ Advocates Limited

The Chambers, 5 Mount Pleasant
Douglas, IM1 2PU
Isle of Man

Tel: +44 1624 626999

Email: caitlin.gelder@dq.im

LinkedIn: www.linkedin.com/in/cait-gelder-583846204



Kathryn Sharman is a senior advisor in DQ's Regulatory & Compliance Services Team. She regularly advises on AML/CFT compliance, in addition to other financial service-related compliance matters.

Kathryn has an LL.B. degree and holds an ICA Anti-Money Laundering Diploma in addition to an ICA Governance, Risk and Compliance Diploma.

DQ Advocates Limited

The Chambers, 5 Mount Pleasant
Douglas, IM1 2PU
Isle of Man

Tel: +44 1624 626999

Email: kathryn.sharman@dq.im

LinkedIn: www.linkedin.com/in/kathryn-sharman-491174153



Sinead O'Connor is Head of Regulatory & Compliance Services for DQ.

Sinead regularly advises on compliance with AML/CFT requirements and provides training to Boards of Directors and others across the financial services sector on their responsibilities under the Isle of Man's AML/CFT framework.

Sinead has spoken in several jurisdictions around the world on AML/CFT and is a member of the Isle of Man AML/CFT Advisory Group.

DQ Advocates Limited

The Chambers, 5 Mount Pleasant
Douglas, IM1 2PU
Isle of Man

Tel: +44 1624 626999

Email: sinead@dq.im

LinkedIn: www.linkedin.com/in/sinead-o-connor-b485222a

DQ Advocates is a leading Isle of Man-based law firm with an international reach.

We offer a full range of legal, regulatory and compliance services to our local and global clients.

DQ is accessible, responsible and commercial, with client-oriented strategies and goals. Our specialist lawyers are recommended as leading lawyers in *Chambers and Partners* and *The Legal 500*.

www.dq.im



Israel



Vered Zlaikha



Ariella May



Shahar Talmon

Lipa Meir & Co.

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The Basic Law of Human Dignity and Freedom 5752-1992, defines the human right to privacy. The principal legislation in Israel is the Protection of Privacy Law, 5741-1981 and the regulations promulgated thereunder (“PPL”). In August 2024, the Israeli Knesset (Israel Parliament) approved the Protection of Privacy Law (Amendment No. 13), 5774-2024 (“Amendment 13”). Amendment 13 will come into effect on August 14, 2025.

Accordingly, all references to the PPL in this document refer to the version of the law as amended by Amendment 13.

1.2 Is there any other general legislation that impacts data protection?

The Communications Law (Bezeq and Transmissions), 5742-1982 – Regulates advertisements via telecommunications systems.

The Consumer Protection Law, 5741-1981 – Includes provisions restricting direct marketing communications (“do not call me” database).

1.3 Is there any sector-specific legislation that impacts data protection?

The Patient’s Rights Law, 5756-1996 – Regulates patients’ rights and health data protection.

The Medical Data Portability Law, 5784-2024 – Regulates the transfer of medical data between medical entities in the healthcare sector and provides that such data may only be transferred with the patients’ consent and while ensuring their privacy.

The Financial Data Services Law, 5781-2021 – Imposes specific obligations on financial institutions, including confidentiality, data deletion and data security requirements.

Additionally, sectoral regulators such as the Supervisor of Banks, the Israel Securities Authority, the Ministry of Health, and the Capital Market Authority, Insurance and Savings regularly issue binding circulars and professional guidelines on data security, applicable to the entities under their supervision.

1.4 What authority(ies) are responsible for data protection?

The Israel Privacy Protection Authority (“PPA”) is the Israeli regulatory and enforcing authority for personal data, in accordance with the PPL.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

As Amendment 13 enters into force on August 14, 2025, all definitions in this section are based on the PPL as amended by Amendment 13.

- **“Personal Data”**
“Detail relating to an identified individual or an individual who can be identified; for the purposes of this definition, ‘an individual who can be identified’ means someone who can be identified with reasonable effort, directly or indirectly, including through an identifying detail such as a name, ID number, biometric identifier, location data, online identifier, or one or more details relating to his/her physical condition, health, economic, social, or cultural status.”
- **“Processing”, “Use”**
“Any action performed on personal data, including its receipt, collection, storage, copying, review, disclosure, exposure, transfer, delivery, or granting access to it.”
- **“Controller”**
“Who determines, alone or jointly with others, the purposes of processing the data in the database, or a body or an officeholder within it authorized by law to process data in a database.”
- **“Processor”**
“Possessor, for the purpose of a database – An external entity to the controller of the database who processes data on the controller’s behalf.”
- **“Data Subject”**
“The individual whose data is contained in the database.”
- **“Sensitive Personal Data”/“Special Categories of Personal Data”**
“Data of Special Sensitivity’ – any of the following:
 1. personal data regarding an individual’s private family life, personal privacy, or sexual orientation;
 2. personal data relating to an individual’s health condition, including medical data as defined in the Patient’s Rights Law, 5756-1996;

3. personal data that is genetic data as defined in the Genetic Data Law, 5760-2000;
4. personal data that is a biometric identifier used or intended for use in electronically identifying a person or verifying their identity;
5. personal data regarding an individual's ethnic origin;
6. personal data regarding an individual's criminal background;
7. personal data regarding an individual's political opinions, religious beliefs, or worldview;
8. personal data that is a personality assessment conducted by a professional in the course of occupation, or by means intended to evaluate essential personality traits, including character, intellectual ability, or work or studies capability;
9. personal data that is location data and traffic data, as defined in the Criminal Procedure (Enforcement Powers – Communications Data) Law, 5767-2007, created by an authorized provider, regarding an individual, and location details that may indicate data under paragraphs (1) to (7) and (11);
10. personal data about an individual's salary data and financial activity;
11. personal data that is designated by law as being subject to confidentiality; or
12. other personal data designated by the Minister of Justice, with the approval of the Constitution, Law and Justice Committee [of the Parliament], in the Second Schedule, provided that it is personal data in a database located in Israel that was transferred from outside the country, and that the jurisdiction from which it was transferred imposes special legal provisions on such types of personal data, compared to those applying to other personal data."

■ **"Severe Security Incident" (i.e. Severe Data Breach)**

"Any of the following:

1. In a database subject to high security level – an incident involving the use of data from the database without authorisation or in excess of authorisation, or damage to the data integrity.
2. In a database subject to medium security level – an incident involving the use of substantial part of the database without authorisation or in excess of authorisation, or damage to the data integrity with respect to a substantial part of the database."²

■ **"Database"**

"A collection of personal data processed by digital means, except for one of the following: (1) a collection for personal use that is not for business purposes; or (2) a collection that includes only names, addresses and contact details, regarding 100,000 individuals or fewer, which does not in itself indicate additional personal data about the individuals listed, provided that the owner of the collection or a corporation under its control does not possess another collection containing other data about the same individuals."

3 Territorial and Material Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

This issue requires a careful case-by-case examination considering the specific circumstances, as it involves issues of the

scope of the PPL, private international law analysis, and taking in account procedural case law developments in Israel, especially regarding multinational corporations.

3.2 Do the data protection laws in your jurisdiction carve out certain processing activities from their material scope?

Yes. Please see definition of "database" above.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

■ **Transparency**

The principle of transparency is embodied in the PPL, which provides that any request for the purpose of collecting personal data from an individual, to be included in or used by a database, must be accompanied by a clear notice specifying whether the individual is legally obligated to provide the data or it is voluntary, the purposes of processing the data, the implications of a refusal to provide personal data, and the intended recipients of the data.

According to a legal opinion of the PPA,³ transparency is a substantive precondition for lawful data processing, and failure to provide a complete and accurate notice may constitute a breach of the law. Moreover, when data processing is based on a legal obligation, the source and nature of that obligation must be clearly disclosed.

The PPA has nevertheless noted in its legal opinion that the extent of detail in fulfilling the duty of disclosure is contextual and may not necessarily require revealing all details. There may be situations where such disclosure is impossible or contrary to legal purposes or other legitimate interests. Then, the entity seeking to balance the different interests must examine how to provide the key information related to the data processing, to allow the data subject to give informed consent to the collection, while avoiding the disclosure of data that cannot be revealed. If it can be assumed that the data subject may not be aware of the data collection or its implications, it is important to ensure that the disclosure is presented as specifically yet comprehensively as possible.

■ **Lawful basis for processing**

The primary legal basis for lawful data processing is informed consent, as defined in the PPL (explicit or implied). Another justification is explicit legal authorisation under the law. As emphasised in the legal opinion of the PPA,⁴ processing personal data without informed consent or explicit legal authorisation may constitute a violation of the law.

■ **Purpose limitation**

The principle of purpose limitation is reflected in the PPL, which requires that when personal data is collected, the data subject must be informed in advance of the specific purpose for which the data is being collected and to whom it may be disclosed.

■ **Data minimisation**

The principle of data minimisation is anchored in the PPL and Data Security Regulations, which require to examine, at least once a year, whether the personal data held in the database exceeds what is necessary for the database's purposes.

■ **Proportionality**

The principle of proportionality requires that the use of personal data does not exceed what is necessary to achieve the intended purpose. Here are some examples:

- In circumstances pointed out by case law within the framework of privacy in labour relations, the processing of data must also meet the requirement of proportionality.
- The PPA Guidance on the Use of Surveillance Cameras also stresses, *inter alia*, that this measure must be proportional, considering location, duration and alternative supervisory tools.
- The PPA draft guidance on AI emphasises that when AI systems are used to process personal data, the scope of processing must be proportionate to the purpose. It also mentions voluntary data protection assessment as a recommended tool to ensure and prove that there is a rational connection between the violation of privacy (in the use of AI) and the fulfilment of the purpose, that there is no alternative with a lesser impact on privacy, and that the expected benefit from the use of the system outweighs the expected harm to the privacy of the data subjects.

■ **Retention**

See “Data minimisation” above.

Also, the Data Security Regulations necessitate in certain circumstances the retention of certain security data details and documentation.

■ **Accuracy**

The accuracy principle is implied through rights granted to data subjects under the PPL, including the right to inspect data held thereof, and the right to request correction of inaccurate, outdated or incomplete data.

Data accuracy is also a component of the Privacy Protection Regulations (Provisions Regarding Data Transferred to Israel from the European Economic Area), 5783-2023, relating to ensuring that the data is accurate, complete, clear and up to date.

■ **Accountability**

Several clauses of the Data Security Regulations reflect how accountability is embedded in Israel data protection laws. These include documentation of processing and risks, maintenance of updated internal policies, performance of audits and extending compliance duties to both controllers and processors.

Additionally, the PPA has issued a Guidance No. 1/2024: The Role of the Board of Directors in Carrying out Corporate Obligations under the Privacy Protection Regulations (Data Security). According to this guidance, the board of directors in a company to which it applies, is required to ensure the existence of a policy for the regulations implementation, and shall define effective mechanisms for supervision, ongoing monitoring and compliance. The board is also required to be involved in supervising specific duties under the regulations.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

■ **Right of access to (copies of) data/data about processing**

According to the PPL, an individual has a right to inspect his/her personal data in a database. Exceptions may

apply when this endangers the data subject’s physical or mental wellbeing, breach legal privilege, or relate to investigations and law enforcement. The PPL also addresses the role of the processor in fulfilling this right.

■ **Right to rectification of errors**

According to the PPL, an individual has the right to request the correction of personal data that is incorrect, incomplete, unclear or outdated.⁵ The controller bears the duty to respond within the timetable stipulated in the regulations thereof.

■ **Right to deletion/right to be forgotten**

The PPL provides an individual (with a limited right in that regard), to request the deletion of personal data if it is incorrect, incomplete, unclear or outdated. The Privacy Protection Regulations (instructions regarding personal data transferred from the EEA to Israel) 5783-2023 widen the scope of deletion duties.

■ **Right to object to processing**

The PPL requires that individuals be informed, at the time of data collection, of the purpose of the processing and of the recipients of the data. This obligation in fact creates an opportunity for individuals to object to specific uses or disclosures of their data.

The PPL also outlines the right of a data subject to restrict the use or transfer of personal data in the context of direct mailing. This includes the ability to request deletion from a direct mailing database and restrict transfer to specific recipients. It may also apply, in certain cases, to the relatives of a deceased individual.

■ **Right to data portability**

■ Policy Paper on the Right to Data Portability (PPA, April 2023) – The PPA, the Israel Competition Authority, the Antitrust Authority and the Consumer Protection and Fair Trade Authority issued a non-binding policy document titled “The Right to Data Portability”, which outlines the conceptual foundations of the right and emphasises its importance.

■ The Medical Data Portability Law, 5784-2024, which was published in August 2024, represents a new sector-specific legislation of data portability in the healthcare sector. It will allow for the secure transfer of medical data between healthcare providers, subject to informed consent of data subjects.

■ Cross-border transfer regulations – Two key regulatory frameworks support portability-related rights in the context of international data flows:

- The Protection of Privacy Regulations (Transfer Abroad, 5761-2001).
- The Regulations regarding personal data transferred from the EEA to Israel (mentioned above).

■ **Right to withdraw consent**

In a recent draft legal opinion on the principle of consent (February 2025), the PPA has suggested that individuals should be able to withdraw consent. According to the PPA’s draft opinion, a principled position recognising the right to withdraw consent – especially in cases of severe privacy violations – has been acknowledged in the rulings of the Supreme Court.

The draft opinion includes further guidance on this, suggesting that in cases where personal data is used based on legally obtained consent, and the individual whose data is being used requests to withdraw consent, this request should be positively considered in certain circumstances.

Moreover, the PPL allows individuals to request removal from direct mailing databases, as specified below.

■ Right to object to marketing

Israeli laws allow individuals to object to the use of their personal data for direct mail as well as for marketing. The PPL allows data subjects to request removal from direct mail databases, limit data transfers, and appeal to court if requests are not met within 30 days. The Communications Law also generally prohibits unsolicited electronic adverts without prior consent (unless certain exceptions are met) and allows individuals to withdraw consent at any time.

■ Right to protect against solely automated decision-making and profiling

The PPA has referred to algorithm-based decision-making systems in its legal opinion on notification (2022). Processing of personal data without sufficient notification, and without the data subject being able to understand what is being done with the data and for what purpose, may constitute a violation of privacy.

The PPA has also issued very recently (April 2025) a draft guidance on AI which emphasises that AI systems should clearly describe how personal data is processed and notify users if the interaction is with an automated system. The more complex the usage, the more detailed the explanation and explicit consent is required.⁶

■ Right to complain to the relevant data protection authority(ies)

According to the PPA website, individuals may submit a query or complaint to the PPA through their website, concerning a potential violation of their privacy. The PPA reviews such complaints and uses them to identify breaches and implement relevant enforcement measures. The PPL stipulates that the PPA would include in its annual report submitted to the Constitution, Law and Justice Committee [of the Parliament], details regarding the number of complaints on controllers' or processors' infringements of the PPL brought before the PPA.

5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

In general, non-profit organisations in Israel are involved in privacy matters, to protect the human right of privacy, especially in relation to legislation and general policies of the government. In some cases, they may also provide concrete legal assistance to data subjects in privacy-related matters.

These non-profit organisations include, *inter alia*, bodies like the Association for Civil Rights in Israel ("ACRI"), Israel Internet Association and legal clinics in leading Israeli universities.

ACRI has filed petitions to the High Court of Justice challenging the governmental use of surveillance technologies during the COVID-19 pandemic (2020). In 2023, ACRI and the Israeli Privacy Association filed a petition against the use of the police surveillance system "Eagle Eye".

6 Children's Personal Data

6.1 What additional obligations apply to the processing of children's personal data?

As elaborated above, data collection and processing are contingent on informed consent as defined in the PPL. Additionally,

the PPA has provided several guidelines and toolkits, including a PPA paper on Protection of Pupil Privacy in Online Remote Learning detailing the privacy guidelines to adopt in schools to protect pupils' privacy.⁷ Also, the PPA has recently issued updated recommendations for parents regarding posting content online that include their children's private data.⁸

7 Registration Formalities and Prior Approval

7.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

Yes. Under the PPL, a database must be registered if one of the following conditions is met: (a) its primary purpose is to collect personal data for the purpose of providing it to others as a business practice or for compensation, including direct mailing services, and the database contains personal data about more than 10,000 individuals; or (b) the controller of the database is a public body (excluding databases of personal data about employees only).

In addition, the PPL stipulates a duty to notify the Registrar if the database contains data of special sensitivity about more than 100,000 data subjects.

7.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

Under the PPL, the details provided should be relatively specific. An application for registration of a database must specify:

1. the identity of the controller and the processor of the database, and their addresses in Israel;
2. the purposes of the database and the objective for which the data is intended;
3. the types of data to be included in the database;
4. particulars on any transfer of data beyond the borders of the state; and
5. particulars on constant receiving data from a public body.

When a duty to notify arises, notification should include the database definitions document and details of the Data Protection Officer ("DPO"), if appointed. The database definitions document under the Data Security Regulations includes description of the details above and further details, such as the main risks concerning a breach of data security and how they are dealt with and the details of the data security officer, if appointed.

7.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

Controllers register their databases (or notify under the revised PPL). Each database that meets the registration criteria must be individually registered.

7.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

Registration applies to any controller whose database meets the registration criteria. In practice, the PPA allows foreign legal entities to appoint an Israeli contact person for communication and compliance purposes in relation to the registration process. The PPA website provides that in relation to a database owned by a foreign company, a database manager who is a foreign resident and citizen shall fill in the registration form with an identification number that is a passport number, provide a physical address, an email address and a phone number of the database owner. Additionally, they must provide a mailing address in Israel.

7.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

See question 7.2 above. Moreover, the registration process at the PPA website refers to specific data of special sensitivity (e.g. cameras data, assessment centres, etc.).

7.6 What are the sanctions for failure to register/notify where required?

In case of failure to register/notify, the PPA can levy monetary sanction of up to 150,000 NIS, and if the database includes personal data of 1 million or more data subjects, the sum can be doubled. Under certain circumstances, this may also result in a court ruling of compensation of 10,000 NIS to an individual, regardless of the damage incurred.

7.7 What is the fee per registration/notification (if applicable)?

This is not applicable.

7.8 How frequently must registrations/notifications be renewed (if applicable)?

In the event of any changes in the details registered or notified, the controller must update the details accordingly, while failure to do so can result in monetary sanctions.

7.9 Is any prior approval required from the data protection regulator?

In cases where there is a legal requirement to register the database, the PPA has a discretion to refuse to register the database or to uphold registration.

The registrar shall register the database within 60 days from the date the application was submitted, unless there has been reasonable ground to believe that the database is used or may be used for illegal activities or as a cover for them, or that the data contained therein was originated, received, accumulated or collected in violation of the PPL or any other legal

provisions. However, if the PPA requests further details from the applicant, the period until the submission of such details shall not be counted within the aforementioned period.

In cases where there is a requirement to notify the PPA, no prior approval is required.

7.10 Can the registration/notification be completed online?

Yes, it can.

7.11 Is there a publicly available list of completed registrations/notifications?

The Databases Registry, which includes certain details of the registered databases, is available to the public. The details available are limited to the name and company number of the controller, the name of the database, the address of the controller, the broad category of data in the database (e.g. “employees”) and the purposes of the database.

7.12 How long does a typical registration/notification process take?

The process can take between a few days and several weeks depending on the complexity. See also question 7.9 above.

8 Appointment of a Data Protection Officer

8.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The appointment of a DPO is mandatory under the PPL in certain circumstances, as follows:

- A controller that is a public organisation, excluding security agencies.
- A controller whose primary purpose is to collect personal data for the purpose of providing it to others as a business practice or for compensation, including direct mailing services, and the database contains personal data about more than 10,000 individuals.
- A controller or a processor whose main activities include data processing, which, due to the nature, scope or purpose, requires continuous and systematic monitoring of individuals, including systematic tracking of a person’s behaviour, location or actions on a significant scale, and among other things, such as mobile phone service providers or online search services.
- A controller or a processor whose main activity includes processing data of special sensitivity on a significant scale, including, among others, banks, insurers, general hospitals and health maintenance organisations.

The PPL also outlines considerations for determining “significant scale” of data processing, which includes, *inter alia*, the number of individuals, the scope and types of data, the duration and frequency of processing activities and the geographical scope of processing, etc.

The PPA has previously issued prior recommendations on DPO (2022), stating that appointing a DPO is voluntarily recommended as a “best practice” to promote compliance and accountability.

8.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

When appointing a DPO is mandatory, the PPA may impose a monetary sanction that is calculated at 2 NIS for every individual whose personal data is in the database. If the database contains data of special sensitivity, the monetary sanction increases to 4 NIS per individual. The PPA could increase the amounts of the sanctions up to at least 20,000 NIS, or 40,000 NIS (the latter for a database containing data of special sensitivity).

8.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

The PPL provides that the DPO must answer directly to the CEO or VP or an officeholder who reports directly to the CEO or VP, and must be free of conflicts of interest. However, there are currently no specific protections from disciplinary measures. The PPA recommendations on DPO (2022) mention that procedures in advance regarding termination of a DPO's term are welcomed.

8.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

The controller/processor must ensure that the DPO has sufficient resources to fulfil his/her duties. Aside from that, the PPL does not include any explicit directives regarding a single DPO covering multiple entities.

8.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The PPL specifies that a DPO must possess the proper knowledge and skills, including:

- In-depth knowledge of privacy protection laws.
- Proper understanding of technology and data security.
- Acquaintance of the organisation's activities and objectives.

The DPO's qualifications should align with the nature, circumstances, scope and purposes of data processing within the organisation.

8.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

The main responsibilities according to the PPL are as follows:

- Serving as the professional authority within the organisation, advising the organisation's management and employees; reporting the management on gaps, with suggestions to correct them.
- Preparing and supervising training programmes, as well as a programmes for ongoing monitoring of compliance.
- Ensuring the existence of data security protocols and database definition documents.
- Handling inquiries from individuals regarding their personal data and rights.
- Serving as the contact person between the entity and the PPA.

8.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

Yes, the above-mentioned notification should include the identity and contact details of the DPO. Additionally, any changes in the identity of the DPO or their contact details must be reported to the registrar within 30 days.

8.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

Yes. The PPL provides that communications with the DPO must be issued publicly in a simple and clear manner.

9 Appointment of Processors

9.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes, the business must enter into a data security agreement with that processor. Additionally, before entering into such an agreement, the business must examine the Data Security risks associated with the engagement.

9.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The above-mentioned agreement should be in writing and cover key issues specified in the Data Securities Regulations, including: the data processed; the technological systems involved; the permitted processing activities; the duration of the agreement; the manner of returning the data to its controller at the end of the agreement; its destruction at the disposal of the external service provider; and of reporting duties to the controller. The agreement must further provide that the processor is required to obtain confidentiality and data security undertakings of the processor's personnel and its sub-contractors and ensure compliance with security measures. The processor should be obliged to report annually on compliance and notify the controller of any security incidents. Control and supervision measures should be put in place to ensure adherence to the agreement and regulations.

10 Marketing

10.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

A database for direct mailing services containing personal data on more than 10,000 individuals requires registration.

A record of the source and date of data collection must be available.

Every approach by direct mail must include, clearly and prominently:

- (1) an indication that such approach is by direct mail, with an indication of the registration number of the database

used for services of direct mail in the registry of the databases;

- (2) a notification of the right of the recipient to be removed from such database attached with the address for that purpose; and
- (3) the identity and address of controller of this database, and the sources from which the controller of the database received that data.

According to the PPL, every individual has the right to demand – in writing – that data related to him be deleted from the database used for direct mailing, as well as to request that personal data not be transferred to any person, group of persons or categories of persons.

The PPL obligates the controller to comply with such a request and to notify the individual in writing that he has done so. The individual has an option to apply to the Magistrates Court if the controller does not respond within 30 days.

Please see also question 10.3 below.

10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

The PPL defines “direct mail” as “an individual approach to individuals, based on their belonging to a population group, determined by one or more characteristics of individuals whose names are included in a database” and “person” is defined as excluding corporations. Nevertheless, if in the business-to-business context the marketing uses an employee’s personal data, the restrictions apply.

10.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

The PPL

The PPL applies to marketing through writing, printed material, telephone, facsimile, computerised means or other methods. These are all subject to the restrictions outlined in the answer to question 10.1.

In a guidance on direct mailing issued by the PPA (February 2017), the PPA refers to an opt-out regime for direct mailing (recipients are included by default unless they explicitly opt out), but the PPA suggests that electronic direct mailing services that are not directly related to the basic (initial) transaction, should be regarded as contingent upon receiving explicit consent from the Data Subject in the form of an opt-in clause.⁹

Consumer Protection Law, 5741-1981

This law establishes a national registry, allowing consumers to register their phone numbers to avoid marketing calls (“do not call me” database).

According to this law, businesses must verify that a number does not appear in the opt-out registry before initiating marketing calls. This obligation is reiterated in the Consumer Protection Regulations (Database for Restricting Marketing Communications), 5782-2022.

The Communications Law (Bezeq and Transmissions), 5742-1982

This law requires generally explicit prior consent before sending marketing messages via fax, automatic dialling

systems, electronic messages or SMS, with the exception that the recipient provided data to the advertiser during the purchase of a product or service, and the advertiser informed the recipient that the details provided would be used for sending advertisements on their behalf; the advertiser gave the recipient the opportunity to notify whether he refuses to receive such advertisements, generally or of a specific type, and the recipient did not do so; the advertisement pertains to a similar product or service as mentioned above.

Exemptions also apply to non-profit organisations and public-benefit companies under certain circumstances.

All advertisements must clearly state these are advertisements, provide the advertiser’s contact information, and offer a simple and immediate opt-out mechanism.

10.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?

There are no explicit restrictions noted above that apply to marketing sent from other jurisdictions. Please see also section 3 above.

10.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

Yes. The PPA has been involved in enforcement of breaches of marketing restrictions (e.g. in relation to parties sending direct emails before elections, or a food provider sending direct emails to customers – in both examples mandatory details did not appear in the emails to the recipients).

10.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Yes. The PPL defines the practice of providing marketing lists to third parties as “direct mailing services”, and the PPA has previously issued “best practices” in that regard. In general, this practice is subject to the PPL requirements, for example – coherency with the purpose of the database and the consent of the data subjects.

10.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

- **Failure to register a database of direct mail services:** 150,000 NIS. If the database contains personal data about 1 million individuals or more, this amount can be doubled.
- **Approaching an individual in violation of the law:** A sanction calculated as 50 NIS (or 100 NIS if the data is of special sensitivity) multiplied by the number of individuals contacted.
- **Avoiding acting in accordance with individual’s request to be removed from a database:** 15,000 NIS.
- **Missing documentation (e.g. for database sources):** 2 NIS per individual, 4 NIS for sensitive data. The PPA could increase the amounts of the sanctions up to at least 20,000 NIS, or 40,000 NIS (the latter for a database containing data of special sensitivity).

11 Cookies

11.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

There is no explicit reference to cookies in Israel primary privacy law. However, the PPA addressed the issue of cookies in its recommendations on privacy in transferring funds and payment apps.¹⁰ In that context, the PPA recommends using an opt-in model to obtain consent from data subjects for cookies usage that is not essential for providing the service.

11.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

The recommendations distinguish between cookies that are essential for providing the service and other cookies.

11.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

Apparently, to date, the PPA has not taken any enforcement action in relation to cookies.

11.4 What are the maximum penalties for breaches of applicable cookie restrictions?

There are no specific penalties. However, should the use of cookies be deemed to have violated notification or consent duties, this may result in sanctions applicable in that regard, for example a sanction calculated as 50 NIS (or 100 NIS if the data is of special sensitivity) multiplied by the number of individuals contacted (or a minimum of 30,000 NIS). As the PPA has so far issued only non-binding recommendations relating to cookies, it remains to be seen what the interpretation of the law in the future would be.

12 Restrictions on International Data Transfers

12.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

The Protection of Privacy Regulations (Transfer of Data Abroad), 5761-2001 (“**Transfer Abroad Regulations**”) stipulate that data from a database in Israel may not be transferred outside its borders unless certain conditions specified are met, including, among others:

1. Data may be transferred to a country whose law ensures a level of data protection that is equivalent to the level of data protection established by Israeli law, all in accordance with the conditions set forth. This includes several key principles, such as: data must be collected and processed lawfully and fairly; purpose limitation; accuracy; the right to inspect and correct personal data; and adequate security measures to protect the data.
2. Data may be transferred under certain conditions, including: the consent of the data subject to the transfer; the transfer of information is required by Israeli law; the data is transferred to a country that is a party to the

European Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), which includes all EU Member States, or a country that has received Adequacy status from the European Union.

12.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

Please see question 12.1 above. There are several additional options, such as transferring data when necessary to protect the health or physical integrity of the individual, or an agreement with the recipient to comply with Israeli data protection requirements (e.g. purpose limitation, data subject rights, confidentiality and data security).¹¹

12.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

The controller is required to include details of international data transfers in the registration form and in the database definition document. Please see above the details of the registration process.

12.4 Do transfers of personal data to other jurisdictions require a transfer impact assessment? If conducting a transfer impact assessment is only mandatory in some circumstances, please identify those circumstances.

The PPL and the regulations thereof do not explicitly require a transfer impact assessment. However, the PPA has issued (2022) a non-binding guiding document recommending that data controllers consider conducting a Privacy Impact Assessment in certain cases, including when data processing involves sensitive personal data, a large-scale transfer or transfers to jurisdictions with lower levels of data protection. While this is not a legal obligation, it reflects emerging best practices encouraged by the PPA.¹²

12.5 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?

The PPA explains at its official website that following *Schrems II*, the PPA issued an updated legal opinion, reiterating that personal data cannot be transferred from Israel to the United States based on the regulation that allows transfers to a country that receives data from European Community Member States under the same conditions. However, the PPA has clarified that when relevant, the transfer of data from Israel to the United States could continue based on the other exceptions of the Data Transfer Regulations (some of those exceptions are elaborated above – see questions 12.1 and 12.2).

12.6 What guidance (if any) has/have the data protection authority(ies) issued in relation to the use of standard contractual/model clauses as a mechanism for international data transfers?

Standard contractual clauses do not apply as such in Israel. The PPA has issued a draft interpretation of the Transfer Abroad Regulations,¹³ which clarifies contractual mechanisms for data transfers, explaining that a controller in Israel may transfer personal data to a foreign entity if the recipient contractually commits to uphold the same conditions that apply to data held in an Israeli database. This includes obligations under Israeli law regarding purpose limitations, data subject rights, confidentiality and data security.

13 Whistle-blower Hotlines

13.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

The PPA Guidance 1/2024 on The Role of the Board of Directors in Carrying out Corporate Obligations under the Privacy Protection Regulations (Data Security) requires boards of directors of relevant organisations (i.e. when processing personal data is of their core business) to ensure the existence of internal oversight mechanisms related to data security, as part of proper corporate governance, although the establishment of a specific reporting hotline is not explicitly mandated.¹⁴

Furthermore, the PPA allows any individual to file a complaint to the PPA regarding a privacy violation through an online form. Complaints may lead to the PPA’s enforcement actions.

13.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

The PPA allows individuals to file complaints anonymously but notes that the absence of identifying details may limit its ability to follow up the complaint.

14 CCTV

14.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

As outlined in the PPA Guidance 4/2012, on the use of CCTV:¹⁵

- Database registration where relevant: any system that includes features such as video recording, footage storage, retrieval capabilities, indexing or automated analysis will typically constitute a “Database” under the PPL. As such, CCTV should be registered in accordance with the PPL requirements.
- Public notice requirement: Organisations using CCTV must inform the public of the existence of the CCTV as a minimum. The notice should be clear and visible (high visibility signs). These signs must clearly state the

purpose of the surveillance and the identity of the entity operating the cameras.

- CCTV in workplaces: The PPA has also issued a dedicated guidance on the deployment of CCTV in workplaces, emphasising the need for necessity, proportionality and transparency when balancing employee monitoring with privacy rights.¹⁶

14.2 Are there limits on the purposes for which CCTV data may be used?

Yes. The purpose of surveillance cameras must be clearly defined, specific and explicit (e.g. for ensuring security and avoiding violence regarding a specific audience, in a defined location). Once the purpose is established, the recordings should not be used for unrelated purposes.¹⁷

According to the PPA Guidance 5/2017 on the use of CCTV in workplaces, the use of surveillance cameras must be for legitimate purposes that are essential to the employer’s business interests or required by law. The data collected should only be used for the specific purposes initially defined, and any use beyond these purposes is generally not permissible, even if the new purpose may be legitimate.¹⁸

15 Employee Monitoring

15.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Employee monitoring is permitted under specific conditions and circumstances, in accordance with case law and PPA guidance.

- Email surveillance – in broad terms, professional email accounts designated for professional use can be monitored by employers if employees are informed and general consent for the employer’s policy is obtained¹⁹ (monitoring is limited to work-related purposes). For dual-use email accounts (both professional and personal purposes), a general consent for the employer’s policy is required, alongside specific consent of the employee for monitoring. Monitoring personal email accounts is prohibited without a court order, and specific consent is needed for each instance of monitoring.
- Attendance systems (using biometric data) – according to the PPA guidance, the use of biometric data for tracking employee attendance is allowed if informed and freely given consent is obtained, with a preference for less intrusive alternatives when possible.²⁰
- Company-owned devices – monitoring is permissible when employees are notified in advance, with a focus on transparency and adherence to principles of reasonableness and proportionality, ensuring that monitoring is confined to legitimate business purposes and does not infringe on personal privacy.

15.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

The consents or notices required are context dependent. Explicit, informed consent is essential for the sensitive practices mentioned above. This can be secured through written employment policies or agreements, and in some cases via direct communication. Policies should be regularly updated to reflect changes and maintain transparency.

15.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

According to the PPA Guidance (5/2017) on CCTV monitoring at workplaces, where possible, employers should engage with works councils, trade unions or employee representatives. This involves consulting them (although it is not necessarily mandatory) about the purpose and scope of CCTV, to ensure transparency,²¹ thus to allow the employer to make an informed and proportionate decision, considering the potential impact on employees and its necessity.

15.4 Are employers entitled to process information on an employee's attendance in office (e.g., to monitor compliance with any internal return-to-office policies)?

Yes.²² This processing is generally permissible if it aligns with legitimate business interests and is conducted in a manner that respects employee privacy. Employers must ensure that such monitoring is reasonable, proportionate and transparent, with employees being informed about the purpose and scope of data collection. Additionally, obtaining informed consent from employees is crucial, especially when using technologies like biometric data for attendance tracking.

16 Data Security and Data Breach

16.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

The PPL stipulates a general obligation to ensure the security of personal data, and the Data Security Regulations stipulate specific duties in that regard. Both the controller and the processor are responsible (while there are limited additional responsibilities of the controller).

16.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Under the Data Security Regulations, in the event of a "severe security incident" (see definition above), the controller must immediately notify the PPA and report the measures taken following the incident. In practice, the PPA reporting form requires the controller to elaborate many details on the database affected as well as the incident, including, *inter alia*, the systems affected, whether sensitive data has been exposed, if other state authorities are involved, whether a ransomware payment demand is involved, if an insurance exists, and more.

16.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

There is no explicit direct regulatory duty to notify affected

data subjects under the Data Security Regulations, though in some cases such duty may be implied from other bodies of law. The PPA may require that the controller notify data subjects who may suffer damage as a result of the incident, after consulting with the Israel National Cyber Directorate (and according to the PPA policy paper, depending on the circumstances, also in coordination with the sectoral regulator). The PPA may direct organisations to do so on a case-by-case basis. In the decision to notify data subjects about a severe security incident, consideration will be given to whether personal data has leaked or if there is merely a risk of leakage, as well as the expected level of harm to the data subjects (such as likelihood that a security incident will lead to identity theft, fraud, or physical or mental harm).

16.4 What are the maximum penalties for personal data security breaches?

The level of monetary sanctions depends on the security level of the database (high, medium or basic). A failure to properly document a security incident can result in a sanction that could reach up to 40,000 NIS for a database of a medium security level, and 160,000 NIS for a database of a high security level. A failure to report a severe security incident can result in a sanction of 80,000 NIS for a database of a medium security level and reach up to 320,000 NIS for a database of a high security level.

17 Enforcement and Sanctions

17.1 Describe the enforcement powers of the data protection authority(ies).

Under the PPL, as it has been revised (Amendment 13), the enforcement powers of the PPA **are significantly enhanced**. In general, the different categories of the PPA powers are as follows:

- (a) **Supervision powers:** e.g. demand identification from related individuals; demand data, documents or computer material related to a database; and enter and search premises.
- (b) **Administrative investigation:** e.g. inquiry, search and seizure of objects under certain circumstances.
- (c) **Sectorial supervision:** prepare a sectorial questionnaire for specific sectors, demand answers and documentation.
- (d) **Administrative enforcement measures:** the PPA may order the controller to cease discrepancies. The order will include the specific breach and the timetable to correct it, as well as the possibility of imposing a monetary sanction if the violation is not ceased.
- (e) **Imposition of administrative sanctions for infringements:** the PPA has the power to impose monetary sanctions for a very wide array of violations, such as processing data in an unregistered database, denying individuals to inspect their personal data, failing to appoint a DPO, or failing to implement adequate security measures to protect personal data from unauthorised access or disclosure. The PPA could alternatively use lesser administrative means, such as Administrative Warning, or a letter of Commitment with guarantees given by the wrongdoer.
- (f) **Judicial restraining order:** the PPA could ask the court to issue a judicial order to cease the processing activities of the database resulting in infringements or suspected to result in infringements, including a judicial order to completely delete the personal data in the database.

- (g) **Criminal investigation:** when a suspicion of an offence of the PPL arises – by an investigator authorised by the head of the PPA.

17.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

There are certain powers that the PPA can exercise with a court order and some it can exercise independently. The PPA holds certain authorities (without a need for a judicial order), such as the **authority to refuse database registration** if there is a reasonable ground to believe it serves illegal activities or contains illegally obtained data. If a database possessor or controller infringes any provision of the law, the PPA may suspend database registration after providing the right to a hearing. **Banning processing activities** requires a judicial order – see question 17.1(g) above.

17.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

In relation to all kinds of PPA powers (described in question 17.1 above) – please see the enforcement trends in question 20.1.

17.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

The PPA has exercised its power against locally incorporated branches of global businesses; however, it has not disclosed any exercise of its powers over businesses established in other jurisdictions.

18 E-discovery/Disclosure to Foreign Law Enforcement Agencies

18.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

- The businesses will typically examine the request taking into account both the PPA and foreign law.
- Formal foreign e-discovery requests or requests for disclosure from foreign law enforcement agencies can be communicated through the government, and those requests are governed by the Legal Assistance Between States Law, 5758-1998. “Legal assistance” under the law includes, *inter alia*, the delivery of documents, collection of evidence, transfer of evidence and other documents, transfer of information, all in connection with a civil or criminal matter. This law provides, in general, that the response to all requests shall comply with Israeli law.
- Nevertheless, the transfer of data as part of the response to the “legal assistance” request falls under the exemption detailed in the Transfer Abroad Regulations as elaborated below in question 18.2.
- Additionally, the PPA has entered into agreements with similar data protection authorities. For example, in April 2025, the PPA signed a Memorandum of Understanding (“MOU”) with the National Privacy Commission of the Philippines. The MOU aims to enhance cross-border cooperation and improve enforcement capabilities

beyond domestic borders. In certain cases, agreements of this kind might also affect handling such requests.

18.2 What guidance has/have the data protection authority(ies) issued on disclosure of personal data to foreign law enforcement or governmental bodies?

In general, the Transfer Abroad Regulations dictate that transfers of personal data should ensure that the recipient country provides a level of data protection that is not less than that provided under Israeli law, or meet other specified criteria. However, the regulations stipulate an exemption for data that is transferred abroad as part of the Legal Assistance Between States Law, 5758-1998.

19 Artificial Intelligence

19.1 Are there any limitations on automated decision-making involving the processing of personal data using artificial intelligence?

Please see question 5.1 above.

19.2 What guidance (if any) has/have the data protection authority(ies) issued in relation to the processing of personal data in connection with artificial intelligence?

The PPA has just recently initiated the “Draft Guidance of the Privacy Protection Authority: Applicability of the Privacy Protection Law to Artificial Intelligence Systems” (April 28, 2025). However, it is important to note that this document is still in draft form and as of the end of June 2025, is still open to comments from the public.

The Draft Guidance defines five criteria that govern the processing of personal data in AI systems:

- Legal basis: that allows for processing personal data that invades privacy during any stage of the AI system’s life-cycle, including training and use.
- Obtaining informed consent: including clear explanations about data collection, AI use and potential risks.
- Transparency: data subjects should be informed about AI operations, including data collection and processing purposes (the level of transparency depends also on the use and complexity of the AI system).
- A data protection impact assessment is recommended to identify and mitigate privacy risks, especially for high-risk AI systems.
- Ensuring data accuracy and allowing for data subjects to request corrections.

20 Trends and Developments

20.1 In your opinion, what enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.

Over the past year, there have been important court rulings as well as a noticeable increase in enforcement activities by the PPA, including the following:

- In May 2025, the PPA announced five enforcement actions taken during that month alone towards organisations of different sectors (including banking, insurance companies, hospitals, non-profit organisations),

regarding infringements of various obligations of the PPL and Data Security Regulations. Those involved severe security incidents, the use of security cameras without proper signage and failure to adequately protect personal data in online services. These actions signal the PPA's intent to intensify enforcement in relation to all sectors and various legal data protection duties.

- In March 2025, the PPA imposed monetary sanctions on EY and PwC branches in Israel for violating the PPL by collecting scans of visitors' ID cards without providing the required notice to obtain consent. The PPA further clarified that, following the entry into force of Amendment 13 in August 2025, the sanctions for such violations are expected to increase significantly.
- In March 2025, the National Labor Tribunal issued an important ruling (NLC 41179-01-24 *Elkaner v. Dr. Mark Friedman Ltd.*), recognising that a violation of privacy through the unproportionate installation of surveillance cameras in the workplace may constitute a "substantial deterioration in employment conditions", entitling the employee to compensation pay upon resignation.
- Following a 2020 cyberattack on Shirbit insurance company, in April 2025, a District Court approved a settlement that Harel insurance company (having acquired Shirbit's operations) will pay approximately 4.9 million NIS in compensation to customers and to the class action fund. This is in addition to a 10 million NIS sanction previously imposed by the Capital Market Authority. The settlement illustrates the growing legal and financial exposure of commercial entities in cases of data breaches.²³
- In June 2025, a class action settlement was approved by the Tel Aviv District Court relating to Bank Discount and users of its PayBox app, following a 2020 data breach. The bank will pay NIS 3.02 million to a dedicated fund for this matter. This settlement has taken into account that PPA has conducted a supervisory procedure, which has indicated some security deficiencies and breaches of the PPL, as well as that the compensation was intended to address emotional harm to some users of the app rather than material damage.

20.2 In your opinion, what "hot topics" are currently a focus for the data protection regulator?

- **Entry into force of the PPL Amendment 13** on August 14, 2025. The Amendment introduces increased enforcement tools for the PPA to apply.
- **The Principle of Consent in Privacy Law** – In February 2025, the PPA issued a Draft Legal Opinion, emphasising the importance of informed consent as a core element of data protection,²⁴ particularly where power imbalances exist or intrusive technologies are used. It has clarified that the consent required differs depending on the context. This is an important trend to follow, as consent is currently the primary basis for data processing under the PPL.
- **The Role of the Board of Directors** – the PPA Guidance on The Role of the Board of Directors in Carrying out Corporate Obligations under the Privacy Protection Regulations (Data Security), clarifies that data security is an integral part of corporate governance, requiring boards of directors to oversee privacy and data security risks, ensure appropriate resource allocation and implement internal control mechanisms.
- **AI** – A Draft Guidance issued by the PPA in April 2025²⁵ sets out proposed guiding principles in relation to privacy and AI technologies as described above. To date, the draft is still open to public comments.

Endnotes

- 1 Clause 1 of the Protection of Privacy Regulations (Data Security) 5777-2017 ("**Data Security Regulations**").
- 2 Clause 1 of the Data Security Regulations.
- 3 PPA publication "Notification Duty while processing personal data", July 2022; PPA publication, "Legal Opinion on the Collection of ID Numbers and Photocopying of ID Cards", March 17, 2024.
- 4 PPA publication, "Legal Opinion on the Collection of ID Numbers and Photocopying of ID Cards", March 17, 2024.
- 5 Privacy Protection Regulations (Conditions for Inspecting Data and Procedures for Appealing Denial of a Request to Inspect), 1981.
- 6 Draft Guidance for Public Comment – Applicability of the Privacy Protection Law to Artificial Intelligence Systems, April 28, 2025.
- 7 PPA Guideline "Student Privacy Guide in Educational Institutions in the Digital Age", November 2021.
- 8 PPA publication "Recommendations on the Disclosure and Sharing of Data about Children Online by Their Parents (Sharenting)", December 18, 2024, updated May 11, 2025.
- 9 PPA Guidance "Guidance – Interpretation and Implementation of the Privacy Protection Law Provisions Regarding Direct Mailing and Direct Mailing Services", June 21, 2017.
- 10 PPA Guidance – Recommendations "Privacy in Apps and Advanced Means for Transferring Funds and Payment in Businesses", April 22, 2021.
- 11 PPA "Draft Legal Opinion on the Transfer of Information Outside of Israel – Interpretation of Regulation 2(4)", July 8, 2024, updated September 15, 2024.
- 12 PPA publication, "Privacy Impact Assessment – Guiding Document", March 2022.
- 13 PPA "Draft Legal Opinion on the Transfer of Data Outside of Israel – Interpretation of Regulation 2(4)", July 8, 2024, updated September 15, 2024.
- 14 PPA Guidance No. 1/2024: The Role of the Board of Directors in Carrying out Corporate Obligations under the Privacy Protection Regulations (Data Security), September 2024.
- 15 PPA Guidance "Use of Security and Surveillance Cameras and Their Image Databases", October 21, 2012.
- 16 PPA Guidance "Guidance for the Use of Surveillance Cameras in the Workplace", October 18, 2017.
- 17 PPA Guidance "Use of Security and Surveillance Cameras and Their Image Databases", October 21, 2012.
- 18 PPA Guidance "Guidance for the Use of Surveillance Cameras in the Workplace", October 18, 2017.
- 19 *Tali Isakov Inbar v. the State of Israel* – The Commissioner for Women's Labour Law".
- 20 PPA Guidance "Policy Document on the Collection and Use of Biometric Data in the Workplace" February 28, 2024.
- 21 PPA Guidance "Guidance for the Use of Surveillance Cameras in the Workplace", October 18, 2017.
- 22 PPA Guidance "Policy Document on the Collection and Use of Biometric Data in the Workplace", February 28, 2024.
- 23 Tel Aviv District Court, Class Action Approval Ruling in re Shirbit Data Breach, CA 6615-12-20 *Azulay et al. v. Shirbit Insurance Company Ltd. et al.* (March 2025).
- 24 PPA publication "Legal Opinion on Consent under Privacy Protection Law – Draft for Public Comments", published February 24, 2025.
- 25 Draft Guidance of the Privacy Protection Authority: Applicability of the Privacy Protection Law to Artificial Intelligence Systems, published on April 28, 2025, updated May 6, 2025.



Vered Zlaikha is a Partner and the Head of the Cyber Affairs & AI Practice at Lipa Meir & Co. Vered is also a member of the Experts Forum advising Israel government on Policy & Regulation of AI. Vered is an expert in Technology Law and Policy. She holds a wealth of experience both at the national and international levels, gained from her previous roles as the Legal Advisor for Technology and Cybersecurity Affairs at the Israel Defence Forces and as the Head of International Cyber Policy and Initiatives at the Israel National Cyber Directorate. Vered represented the State of Israel at the UN OEWG (Open-Ended Working Group), on cybersecurity affairs. She was a Vice-Chair and Bureau Member of the Working Party on Security in the Digital Economy at the OECD.

Vered provides legal advice to a broad range of clients of all sectors, both public and private entities, including technology companies, financial & insurance companies, the healthcare sector, the automotive industry and other industries. She represents legal positions at the Knesset (Israel Parliament) and before regulators, leads contract negotiations and provides extensive legal advice pertaining to AI systems, cyber incidents, and privacy and data protection regulations, both in connection with transactions (including due diligence aspects) as well as regulatory interfaces. In recent years, she has been serving as a Research Fellow at the Hebrew University – Federmann Cybersecurity Research Center, as a Board Member at the Israel Internet Association (ISOC-IL), and as a member of the steering committee of the Haifa University Cyber Law and Policy Research Center. Vered holds an LL.M. from Tel Aviv University, *magna cum laude* (2006) and an LL.B. from Bar Ilan University (2000). She also holds an M.A. from Tel Aviv University, in the Executive Program for Political Science, Diplomacy & Security (2012). She is a certified Lawyer of the Israel Bar Association (2000).

Lipa Meir & Co.
Beit Amot Investments Tower, 2 Weizmann St. Tel-Aviv
Israel

Tel: +972 3607 0600
Email: veredz@lipameir.co.il
LinkedIn: www.linkedin.com/in/vered-zlaikha-8aa95633



Ariella May is a Legal Intern at Lipa Meir & Co., where she brings together her strong legal foundation with a keen interest in technology and AI. Before starting her internship, Ariella worked as a Legal Data Specialist at Darrow AI, a legal tech startup that uses AI to detect large-scale legal violations. This role required both legal acumen and technological fluency, positioning her at the forefront of AI's integration into legal practice.

Ariella earned her LL.B. (Bachelor of Laws) from Bar-Ilan University, one of Israel's leading law faculties, where she gained solid training in both theoretical and applied legal principles. She is a native English speaker, further enhancing her ability to navigate international legal contexts, collaborate across borders and engage with global legal-tech discourse.

Lipa Meir & Co.
Beit Amot Investments Tower, 2 Weizmann St. Tel-Aviv
Israel

Tel: +972 3607 0600
Email: ariellam@lipameir.co.il
LinkedIn: www.linkedin.com/in/ariella-may-72b25b211



Shahar Talmon is a dedicated legal professional currently serving as a Legal Intern at Lipa Meir & Co. In her role within the Technology, Corporate & M&A Department, Shahar is gaining invaluable experience in the dynamic intersection of law and technology. Prior to her current position, Shahar served as a Pre-Intern at another Israeli law firm, where she worked in the Litigation and Insolvency Departments, dealing with intricate legal disputes and financial restructurings. Additionally, she gained firsthand experience in the judicial system as a Judicial Clerk Assistant at the Administration of Courts, assisting a civil judge at the Magistrate's Court. Her international exposure includes participating as a delegate for the Israeli German Lawyers Association at the 27th Annual Conference with the German Bar Association in Frankfurt, focusing on constitutional law, international law and human rights.

Lipa Meir & Co.
Beit Amot Investments Tower, 2 Weizmann St. Tel-Aviv
Israel

Tel: +972 3607 0600
Email: shahart@lipameir.co.il
LinkedIn: www.linkedin.com/in/shahar-talmon-52a294344

Lipa Meir & Co. stands as one of Israel's premier law firms, delivering comprehensive civil, corporate and commercial legal services to both domestic and multinational clients. With a team of approximately 80 attorneys, the firm has established itself as a leading destination for businesses seeking personal, professional and creative legal solutions. The firm operates through specialised departments: Commercial Law, Litigation and Dispute Resolution; Technology; Corporate M&A; Real Estate and Finance; Real Estate Hotels & Leisure; and Employment Law. This structured approach enables the firm to provide focused expertise across diverse legal areas while maintaining the highest standards of service quality. Lipa Meir & Co.'s reputation extends beyond Israel's borders, earning recognition from prestigious international legal ranking guides including *Chambers & Partners*, *The Legal 500*, *IFLR 1000*, *WTR1000*, *BDI*, and *Dun's 100*. This international acclaim reflects the firm's commitment to excellence and its position at the forefront of

Israel's legal landscape. The firm's global perspective sets it apart, with attorneys who have studied, trained and worked overseas, bringing invaluable international experience to their practice. This expertise enables them to effectively serve clients operating across various jurisdictions, including the United States, Europe, Asia and Latin America, facilitating both Israeli companies' international expansion and foreign investment in Israeli markets.

www.lipameir.co.il



Japan

Japan



Hiromi Hayashi



Masaki Yukawa

Mori Hamada & Matsumoto

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The principal data protection legislation is the Act on the Protection of Personal Information (Act No. 57 of 2003; the “APPI”), which applies to both the public and the private sectors.

The Personal Information Protection Committee (the “PPC”), which is the main agency that enforces the APPI, issues general guidelines on the implementation of the APPI. Guidelines that apply specifically to certain industries (e.g., financial, healthcare and telecommunication sectors) are jointly issued by the PPC and the competent government body that supervises the relevant industry.

APPI

It is the APPI’s basic principle that the cautious handling of personal information (see question 2.1 for the definition), under the principle of respect for individuals, will promote the proper handling of personal information (APPI, Article 3).

Chapters 2 and 3 of the APPI set forth the basic frameworks of the responsibilities and policies of the national and local governments to protect personal information. Pursuant to Article 7 of the APPI, the Cabinet established the “Basic Policy on the Protection of Personal Information” (*Kojin Jyouchou no Hogo ni kansuru Kihon Houshin*) in 2004 (as amended; the “Basic Policy”).

Chapter 4 regulates the use of personal information by private businesses and sets forth the obligations of “Business Operators Handling Personal Information” (*Kojin Joho Toriatsukai Jigyosha*) (the “handling operators”), as defined in Article 16, paragraph 2 of the APPI. Any business operator using a personal information database (please see question 2.1 for the definition) is considered a handling operator regardless of the scale of its personal information database. Chapter 4 also regulates person-related information, pseudonymised information and anonymised information (see question 2.1 for the definitions).

Chapter 5 regulates the handling of personal information by administrative organs and independent administrative agencies.

Privacy Mark

A business operator may use a logo called a “Privacy Mark” (the “Privacy Mark System”) issued by the Japan Information Processing Development Center to certify its compliance with

the relevant laws and the Japan Industrial Standards (“JIS Q 15001”). JIS Q 15001 is not a law; however, in certain aspects, it provides a higher level of standards than the APPI. The most updated version of JIS Q 15001 is the 2023 version.

1.2 Is there any other general legislation that impacts data protection?

(a) Privacy right

The right to privacy is recognised by Japanese courts as an individual’s right to keep their private life private, and for their private life not to be disclosed without a legitimate reason. This is recognised among academics as the right to control one’s own personal information. Therefore, in addition to complying with the APPI, a person who possesses the personal information of others in Japan must not infringe on the privacy rights of the principals.

(b) Privacy of communications

Article 4 of the Telecommunications Business Act provides that no person may infringe on the privacy of the communications handled by telecommunications business operators. The privacy of communications does not necessarily refer to personal information, although the guidelines issued by the Ministry of Internal Affairs and Communication (“MIC”) for the protection of personal information in the telecommunication business (please see question 1.3) also deal with the privacy of communications, such as telecommunications logs (the “MIC Guidelines”).

(c) Electronic mail

The Act on the Regulation of the Transmission of Specified Electronic Mail (Act No. 26 of 2002; the “Anti-Spam Act”) regulates unsolicited marketing by email. Please see question 9.1.

(d) Specified commercial transactions

The Act on Specified Commercial Transactions (Act No. 57 of 1976) regulates, among other forms of unsolicited marketing, unsolicited marketing by email. Please see question 9.1.

(e) Utilisation of numbers to identify individuals in administrative procedures

The Japanese government adopted a social security and tax number system and, in 2015, assigned specific numbers to entities and individuals pursuant to the Act on the Utilisation of Numbers to Identify Specific Individuals in Administrative Procedures (Act No. 27 of 2013; the “Individual Number Act”). The collection, provision and use of the numbers assigned to individuals

are allowed only for statutorily provided purposes (such as submission of tax notifications) and may not be used for other purposes.

(f) **Telecommunications Business Act**

The Telecommunications Business Act provides (a) requirements to protect information that can identify users (such as access log data) applicable to large-scale telecommunications service providers (please see question 1.3 and section 8), and (b) requirements for the use of third-party cookies or otherwise transmitting information to third-party servers (please see section 11).

1.3 Is there any sector-specific legislation that impacts data protection?

The PPC was established in 2016 as the main agency that will enforce and apply the APPI. While the PPC issues general guidelines on the implementation of the APPI (the “**PPC Guidelines**”), the PPC also issued certain sector-specific guidelines jointly with other ministries, such as: (a) telecommunications sector guidelines issued jointly with the MIC; (b) broadcasting sector guidelines issued jointly with the MIC; (c) postal service sector guidelines issued jointly with the MIC; (d) genetic information business guidelines issued jointly with the Ministry of Economy, Trade and Industry; (e) financial sector guidelines issued jointly with the Financial Services Agency; and (f) medical sector guidelines issued jointly with the Ministry of Health, Labour and Welfare.

Under the Telecommunications Business Act, telecommunications service providers with 10 million or more users (for free-of-charge services) or 5 million or more users (for paid services) will be designated as large-scale telecommunications service providers by the MIC. If so designated, they must (i) establish information protection procedures and submit them to the MIC within three months from the designation, (ii) disclose information protection policies within three months from the designation, (iii) appoint an information protection officer and notify the MIC of the appointment within three months from the designation, (iv) annually review compliance with the said information protection procedures and policies, data breaches, and other matters regarding information protection, and (v) report certain data breaches (please see question 2.1) to the MIC.

1.4 What authority(ies) are responsible for data protection?

The PPC, as an independent regulatory body, is authorised to advise a handling operator or require it to prepare and submit a report on the handling of personal information to the extent necessary to implement the APPI (APPI, Articles 146 and 147). If a handling operator violates the APPI, the PPC may urge it to cease the violation and take other necessary measures to correct the violation (*id.* Article 148, paragraph 1). If the PPC finds it necessary and certain requirements are met, it may order the handling operator to take the urged measures or to cease the violation and take other necessary measures to rectify the violation (*id.* Article 148, paragraphs 2 and 3).

The PPC is also responsible for the supervision and enforcement of the Individual Number Act (Article 33).

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **“Personal data”**
The APPI provides for four definitions relevant to personal data:
 - **“Personal information”** is information about living individuals that (a) can identify specific individuals, or (b) contains an “individual identification code”. Information that can identify specific individuals under clause (a) of the definition includes information that can be readily collated with other information to identify specific individuals.
The “**individual identification code**” under clause (b) of the definition of “personal information” above refers to any character, number, symbol or other code (i) into which certain body features (such as DNA, appearance and fingerprints) of a specific individual have been converted by computers for use and which can identify such specific individual, or (ii) which is assigned to individuals (such as a driver’s licence number, number assigned under the Individual Number Act, and passport number) (APPI, Article 2, paragraphs 1 and 2).
 - **“Personal information database”** means an assembly of information including the following: (a) an assembly of information systematically arranged in such a way that specific personal information can be retrieved by a computer; and (b) an assembly of information designated by a Cabinet Order as being systematically arranged in such a way that specific personal information can be easily retrieved. However, any assembly of information the use of which is not likely to harm the interests of the individual principals, as further set out in the Cabinet Order of the APPI, is excluded from the definition (*id.* Article 16, paragraph 1).
 - **“Personal data”** means personal information constituting a personal information database (*id.* Article 16, paragraph 3).
 - **“Retained personal data”** means personal data that a handling operator has the authority to disclose, correct, add, erase or delete, discontinue its utilisation or discontinue its provision to a third party. However, it excludes any personal data the existence or absence of which would harm the life, body or property of the relevant individual or a third party, encourage or solicit illegal or unjust acts, jeopardise the safety of Japan or harm the trust of or negotiations with other countries or international organisations, or impede crime investigations or public safety (*id.* Article 16, paragraph 4).
- **“Processing”**
The APPI does not define “processing”. Although the APPI uses certain words such as handling (*toriatsukai*), collection (*shutoku*), use (*riyou*), provisions (*teikyo*) to third parties and disclosure (*kaiji*), it does not define these words.
- **“Controller”**
Please see the definition of “processor” below.
- **“Processor”**
The APPI does not use “controller” or “processor”. However, a handling operator (*Kojin Joho Toriatsukai*

Jigyosha) may be comparable to a controller or a processor in that it is subject to obligations to protect personal information. Please see question 1.1 for the definition of a handling operator. Foreign companies doing business in Japan will be regulated as handling operators if they fall within the definition.

- **“Data subject”**

The term “principal” would be comparable to a “data subject”. Article 2, paragraph 4 of the APPI defines “principal” as a specific individual identified by personal information.

- **“Sensitive personal data”**

“Sensitive personal data” is defined in the APPI as data referring to race, creed, social status, medical history, criminal record, whether one has been a victim of crime, and other personal information which needs careful handling so as not to cause social discrimination, prejudice or other disadvantages (APPI, Article 2, paragraph 3). The Cabinet Order for the APPI provides details of what constitutes sensitive personal data, which include: physical or mental disabilities; results of medical examinations conducted by doctors or personnel who are engaged in medical services; records of medical treatment or medical advice provided based on the results of medical examinations or due to a disease, an injury or other changes in physical or mental conditions; and history related to criminal procedures such as arrest, investigation or detention.

Under the financial sector guidelines, handling operators in the financial sector must treat not only sensitive personal data, but also labour union membership status, family origin, domicile of origin, healthcare and sex life, which are not expressly included in the foregoing scope of sensitive personal data, as sensitive personal data.

- **“Data breach”**

“Data breach” is not a term under the APPI; however, certain designated incidents of leakage of, loss of, and damage to personal data must be reported to the PPC. Reportable incidents include: (a) actual or suspected leakage of, loss of, or damage to personal data including sensitive personal data; (b) actual or suspected leakage of, loss of, or damage to personal data which can be abused for economic gains; (c) actual or suspected leakage of, loss of, or damage to personal data caused by a malicious act; and (d) actual or suspected leakage of, loss of, or damage to personal data where more than 1,000 principals are affected. Under an APPI amendment, which took effect in April 2024, an actual or suspected leakage of, loss of, or damage to personal information before it is incorporated into a database (that is, before it is considered personal data) due to a malicious act (such as information provided online being stolen before it is entered into a database) must now also be reported.

In addition, under the Telecommunications Business Act, the data breaches that must be reported to the MIC are any leakage of information that is (i) protected by the secrecy of communication, (ii) not protected by the secrecy of communication but where more than 1,000 users are affected, or (iii) not protected by the secrecy of communication but where such information was seized by a foreign government pursuant to a foreign law.

- **“Anonymised information”**

“Anonymised information” is defined as information obtained by removing or replacing with random descriptions certain parts of personal information such that any

specific individual cannot be identified by any means and the original personal information cannot be restored (APPI, Article 2, paragraph 6). Anonymised information is not regulated as personal information since it does not identify any individual, but certain regulations apply, such as anonymising personal information in accordance with the PPC ordinance and guidelines and the prohibition against restoring personal information.

- **“Pseudonymised information”**

“Pseudonymised information” is defined as information obtained by removing or replacing with random descriptions certain parts of personal information such that any specific individual cannot be identified unless collated with other information (APPI, Article 2, paragraph 5). Pseudonymised information may also be regulated as personal information if a removed or replaced part is retained so that a specific individual can be identified if collated with other information; however, pseudonymised information is exempted from certain regulations. For example, pseudonymised information can be used for new purposes not notified to data subjects at the time of collection even if the new purposes are not related to the original purposes. This deregulation was introduced in April 2022 to promote data economy.

- **“Person-related information”**

“Person-related information” is defined as any information related to any living individual other than personal information, anonymised information or pseudonymised information (APPI, Article 2, paragraph 7). This definition is broad, but most practically applies to cookies, IP addresses and device IDs, which are collected at websites and applications without user logins. The regulation of person-related information was introduced in April 2022 to require the consent of principals to allow cookies or provide IP addresses and device IDs to third parties which associate those types of information with other information to identify principals.

3 Territorial and Material Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The APPI also applies to business operators outside Japan, without regard to where they were established, if they handle personal information of individuals located in Japan in connection with the provision of goods or services to individuals located in Japan (APPI, Article 171).

3.2 Do the data protection laws in your jurisdiction carve out certain processing activities from their material scope?

The APPI defines a handling operator that is subject to APPI obligations as a business operator which uses a personal information database for business. Thus, collecting or using personal information for a personal purpose is not within the scope of the APPI. Also, collecting or using personal information for press, literary, religious or political purposes are exempted from obligations under the APPI (please see “Exceptions” in question 4.1).

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
The APPI has no provision explicitly dealing with transparency. However, handling operators are required to either publicly announce or notify the principals of the purposes of use of their personal information promptly after the collection of personal information (subject to certain exceptions) (APPI, Article 21). Further, the basic policy requires handling operators to establish and publicly disclose their privacy policy or privacy statement, as well as their use of service providers to handle collected personal information and the extent of the service.
- **Lawful basis for processing**
Handling operators are prohibited from collecting personal information by deception or other wrongful means (*id.* Article 20). Handling operators are also prohibited from collecting sensitive personal information without the consent of the principal except:
 - (a) if required by laws and regulations;
 - (b) if necessary to protect the life, body or property of a person and it is difficult to obtain the consent of the principal;
 - (c) if necessary to improve public health and promote the sound nurturing of the young and it is difficult to obtain the consent of the principal;
 - (d) if necessary for governmental bodies to perform their business and getting the consent of the principal will likely impede the proper performance of business;
 - (e) if the handling operator is an academic research institute and the acquisition is necessary for an academic research purpose;
 - (f) if acquired from an academic research institute and the acquisition is necessary for an academic research purpose;
 - (g) for sensitive personal information that has been disclosed to the public by the principal, governmental bodies or certain parties designated by the PPC (e.g., foreign governments and international organisations);
 - (h) if the sensitive personal information is apparent from the appearance of the principal and is collected through observation or video recording (e.g., a surveillance camera records a person using a wheelchair); or
 - (i) if received from third parties as an entrustment of personal data, through a merger or other business reorganisation, or as joint use.
- **Purpose limitation**
Handling operators are required to specify the purposes of use of personal information to the extent possible and not to use the personal information of any person, without obtaining the prior consent of that person, beyond the scope necessary to achieve the specified purpose of utilisation of personal information (*id.* Articles 17 and 18). Further, handling operators are required to endeavour to keep personal data accurate and up to date within the scope necessary to achieve the purpose of use of personal information (*id.* Article 22).
- **Data minimisation**
The APPI has no provision on data minimisation.

- **Proportionality**
The APPI has no provision on proportionality.
- **Retention**
Handling operators are required to endeavour to delete personal data if it becomes unnecessary (*id.* Article 22). Further, there may be other restrictions under industry-specific guidelines. For example, the MIC Guidelines provide that telecommunication business operators must define their retention period for personal data, which must be within the period needed for the purposes of use, and must endeavour to erase personal information without delay after the expiration of the retention period (MIC Guidelines, Article 11).
- **Restriction on provision of personal data to a third party**
A handling operator is prohibited from providing personal data to a third party without obtaining the prior consent of the principal, subject to certain exceptions (APPI, Article 27, paragraph 1), such as an “opt-out” arrangement under which the handling operator:
 - (a) agrees to stop providing the personal data to the third party upon the demand of the principal; and (b) notifies the principal and the PPC of the following details:
 - (i) the name, address and name of representative of the handling operator;
 - (ii) a statement that the provision to third parties is included in the purposes of use;
 - (iii) the items to be provided to third parties;
 - (iv) how the personal data is collected;
 - (v) how the personal data is provided to third parties (e.g., by publishing a book or uploading to a website through the internet);
 - (vi) a statement that the handling operator will stop the provision if requested by the principal;
 - (vii) how the principal can request the cessation of the data provision (e.g., telephone, email or by written means);
 - (viii) how the personal data is updated; and
 - (ix) when the “opt-out” arrangement starts (*id.* Article 27, paragraph 2).It should be noted that this “opt-out” arrangement is not allowed for the provision of:
 - (1) any sensitive personal data;
 - (2) any personal data collected in breach of the APPI; and
 - (3) any personal data obtained through another “opt-out” arrangement.The PPC proposes to impose additional requirements for “opt-out” arrangements.
- **Exceptions**
The obligations imposed on handling operators will not apply to handling operators that fall under any of the following items and if all or part of the purpose of handling personal information is prescribed in the following applicable items (*id.* Article 57):
 - (a) broadcasting institutions, newspaper publishers, communication agencies and other forms of the press (including individuals engaged in news reporting as their business); for the purpose of news reporting;
 - (b) business operators in the business of literary work; for the purpose of literary work;
 - (c) religious organisations; for the purpose of religious activities (including activities incidental thereto); or
 - (d) political organisations; for the purpose of political activities (including activities incidental thereto).Prior to April 2022, universities and other organisations or groups aimed at academic studies, and persons belonging to those organisations or groups, were also exempted from the APPI to the extent that they handle personal data for the purpose of academic studies. However, due to this exemption from the APPI, academic data transfers from EEA countries to Japanese universities and other

academic institutes for academic research purposes were excluded from the adequacy decision of the European Commission in January 2019. In order to enable the foregoing excluded data transfers from EEA countries, in April 2022, APPI became applicable to academic institutes for academic research purposes with regard to security measures and principals' rights. However, universities and other academic institutes continue to be exempted from the purposes of use restriction, prohibition on sensitive personal information collection, and provision of personal data to third parties.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

■ Right of access to data/copies of data

A handling operator is required to make accessible to the principals certain information (such as the name, address and name of representative of the handling operator, the purposes of use of personal information, how principals can exercise their rights, security measures that the handling operator takes, and how the principals can bring claims) regarding retained personal data (APPI, Article 32, paragraph 1).

Further, at a principal's request, a handling operator must notify the principal of the purposes of use of retained personal data (*id.* Article 32, paragraph 2), subject to the following exceptions:

- (a) the purposes of use are evident from the information made available to the principal by the handling operator pursuant to Article 32, paragraph 1 of the APPI;
- (b) disclosure of the purposes of use is likely to harm the life, body, property, or other rights or interests of the principal or a third party;
- (c) disclosure of the purposes of use is likely to harm the rights or legitimate interests of the handling operator; or
- (d) disclosure of the purposes of use is likely to impede the handling operator's cooperation with the national or a local government.

In addition, the handling operator is required to disclose, without delay, and upon the request of an individual, that person's Retained Personal Data, subject to certain exceptions (*id.* Article 33), subject to the following exceptions:

- (i) disclosure will likely harm the life, body, property, or other rights or interests of the person or a third party;
- (ii) disclosure will likely seriously impede the proper execution of the business of the handling operator; or
- (iii) disclosure will violate other laws and regulations.

A principal may specify, from among a mobile communication, an email or other means of telecommunication, how the retained personal data will be disclosed to the principal. In principle, the handling operator must provide the data by the specified means; however, the handling operator may provide the data in hard copy if the specified means is excessively costly or is otherwise difficult.

The handling operator may charge a fee for complying with a request to notify the purpose of utilisation pursuant to Article 32, or to disclose retained personal data pursuant to Article 33.

■ Right to rectification of errors

The principal may request the handling operator to correct, add or delete retained personal data if the retained personal data are not correct. The handling operator must investigate without delay and, based on the results of the investigation, correct, add or delete, as requested by the principal, the retained personal data to the extent necessary to achieve the purposes of use (*id.* Article 34).

■ Right to deletion/right to be forgotten

As above, the principal may request the handling operator to correct, add or delete retained personal data if the retained personal data are not correct. There is no explicit legal provision on the "right to be forgotten".

■ Right to object to processing

The principal may request a handling operator (a) to discontinue the use of, or erase, retained personal data, and (b) to stop providing the retained personal data to third parties if such use or disclosure is or was made, or the retained personal data in question was obtained, in violation of the APPI. The handling operator must discontinue the use of, or the provision to third parties of, or erase, retained personal data upon the request of the principal if the request has reasonable grounds (*id.* Article 35).

In addition, the principal may request a handling operator to (a) discontinue the use of the retained personal data, and (b) stop providing the retained personal data to third parties if the handling operator ceases to have any reason to use the retained personal data, a material data breach has occurred, or the right or legitimate interest of the principal may be harmed by any other reason.

However, these obligations will not apply if it will be excessively costly or difficult to discontinue the use of, or to erase, the retained personal data and the handling operator takes necessary alternative measures to protect the rights and interests of the principal.

■ Right to restrict processing

There is no "right to restrict processing" which differs from the rights stipulated above in "right to object to processing".

■ Right to data portability

The APPI does not grant a right to data portability. However, the MIC Guidelines require telecommunications service providers to provide information about data portability in their privacy policy.

■ Right to withdraw consent

There is no explicit stipulation regarding the right to withdraw consent under the APPI.

■ Right to object to marketing

There are no provisions explicitly setting forth objections to marketing in the APPI, but business operators must not use personal information for marketing in certain cases. Under the financial sector guidelines, a principal may request handling operators in the financial sector to stop sending marketing materials using personal information collected in connection with loans and other credit provisions. Please see question 10.1 for restrictions on e-mail marketing.

■ Right to complain to the relevant data protection authority(ies)

Individuals may complain to the PPC, and the PPC will conduct necessary mediation regarding a lodged complaint (*id.* Article 129(ii)).

■ **Complaint to Authorised Entities for Protection of Personal Information (*Nintei Kojin Jyouchou Hogo Dantai*)**

Authorised Entities for the Protection of Personal Information (*Nintei Kojin Jyouchou Hogo Dantai*) (“**Authorised Entities**”) are entities authorised by the PPC to handle complaints from individuals on the handling of personal information by their respective member handling operators (“**member handling operators**”). As of 7 April 2025, 41 entities have obtained such authorisation.

When an Authorised Entity is requested by an individual to resolve a complaint about the handling of personal information by a member handling operator, it must promptly notify the member handling operator of the complaint and give necessary advice, investigate the circumstances pertaining to the complaint and request the member handling operator to resolve the complaint promptly. It may, if necessary, request the member handling operator to explain in writing or orally, or request it to submit relevant materials. The member handling operator may not reject such request without a justifiable ground (*id.* Article 53).

5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

The APPI does not grant individuals the right to mandate non-for-profit organisations to seek remedies on their behalf or seek collective redress. However, separately from the APPI, there is a procedural law titled the Act on Special Measures Concerning Civil Court Proceedings for Collective Redress for Property Damages Incurred by Consumers, which allows certified consumer groups to seek, on behalf of consumers, collective redress for damages. Such collective redress has not been used for data breach cases since it used to be limited to the recovery of property damages and could not be used for emotional damages. However, the scope of the said Act was broadened to cover emotional damages as well in October 2023. Furthermore, the PPC Paper proposes to introduce a collective injunction and redress scheme specifically for the breach of the APPI.

6 Children’s Personal Data

6.1 What additional obligations apply to the processing of children’s personal data?

The APPI does not set special rules for the handling of children’s personal data. With regard to consent capacity under the APPI, the PPC guidelines clarify that, if minor principals under the age of 18 are not capable of understanding the consequences of consent, the consent of a statutory representative (parent or guardian) must be obtained where the principal’s consent is required under the APPI. The PPC proposes to introduce special rules for children’s personal data.

7 Registration Formalities and Prior Approval

7.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

The APPI imposes no requirement on a handling operator to register or notify the PPC to process personal information. However, if the handling operator provides personal information to third parties without obtaining the prior consent of the principals under an “opt-out” arrangement, it is required to notify the PPC (please see question 4.1).

The PPC is also authorised to enter offices or other places, to make inquiries and investigate, and to require a handling operator to report or submit materials regarding the handling of personal information, pseudonymised information, anonymised information or person-related information, to the extent necessary to implement the APPI (*id.* Article 146). Please see question 1.4.

7.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

Please see question 7.1.

7.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

Please see question 7.1.

7.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

Please see question 7.1.

7.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

Please see question 7.1.

7.6 What are the sanctions for failure to register/notify where required?

Please see question 7.1.

7.7 What is the fee per registration/notification (if applicable)?

Please see question 7.1.

7.8 How frequently must registrations/notifications be renewed (if applicable)?

Please see question 7.1.

7.9 Is any prior approval required from the data protection regulator?

Please see question 7.1.

7.10 Can the registration/notification be completed online?

Please see question 7.1.

7.11 Is there a publicly available list of completed registrations/notifications?

Please see question 7.1.

7.12 How long does a typical registration/notification process take?

Please see question 7.1.

8 Appointment of a Data Protection Officer

8.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The APPI has no provision mandating the appointment of a privacy or data protection officer (“DPO”). However, the handling operator is required to take necessary and proper measures for the prevention of leakage, loss or damage, and for other security control of personal data (APPI, Article 23). Under the PPC Guidelines, those measures should include the following:

- (a) organisational security measures, such as establishing rules for handling personal data, and specifying the person responsible for supervising the handling of personal data;
- (b) human resource security measures, including the education of employees;
- (c) physical security measures, including controlling the area where personal data is handled, such as servers and offices;
- (d) technical security measures, including controlling access to personal data; and
- (e) having an understanding of the relevant country’s environment if data is handled outside Japan.

The PPC Guidelines indicate that appointing a person to be in charge of the handling of personal data is an example of a proper and necessary measure.

Separately from the APPI, as discussed in question 1.3, large-scale telecommunications service providers designated by the MIC will be required to appoint an information protection officer and notify the MIC of the appointment.

8.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

Although a handling operator is expected to adopt the measures described in the PPC Guidelines, the failure to adopt such measures is not a direct breach of the APPI.

The failure of large-scale telecommunications service providers to appoint an information protection officer is punishable by a fine of up to 2 million yen.

8.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

The APPI does not offer any special protection. However, Article 27-11, Paragraph 2 of the Telecommunications Business Act provides that the opinion of the information protection officer must be respected. Also, the MIC must be informed of the dismissal of that officer.

8.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

Since neither the APPI nor the Telecommunications Business Act requires an information protection officer to be devoted to one entity, multiple entities may appoint the same person for that position.

8.5 Please describe any specific qualifications for the Data Protection Officer required by law.

There are no requirements under the APPI. However, the Telecommunications Business Act requires a DPO to have (i) management level responsibilities, and (ii) at least three years of experience in data protection or compliance or equivalent.

8.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

Please see question 8.1.

8.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

The APPI does not require registration/notification. However, the Telecommunications Business Act requires that the MIC be notified of the appointment and dismissal of a DPO.

8.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

There is no requirement in the APPI for a DPO to be named in a public notice. However, the privacy notice must disclose the name of the director who has capacity to represent the handling operator (e.g., CEO).

There is no requirement in the Telecommunications Business Act to disclose the name of the DPO to the public.

9 Appointment of Processors

9.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

There is no concept of “processor” under the APPI (please see question 2.1). However, there is a concept of “entrustment” of the handling of personal data in which entering into an agreement is recommended.

Under Article 27, paragraph 5(i) of the APPI, if the handling operator entrusts all or part of the handling of the personal data it acquires to an individual or another entity, that individual or entity will not be considered a “third party” under Article 27, paragraph 1.

For example, if the handling operator uses third-party vendors for services, and it shares personal data with those third-party vendors for them to use on the handling operator’s behalf, and not for their own use, such transfer will be deemed an “entrustment” and the restriction on the provision of personal data to a third party under Article 27 will not apply. Please note, however, that the restriction on cross-border transfers under Article 28 still applies when entrusting personal data to a third-party service provider outside Japan (see question 12.1).

When the handling operator “entrusts” personal information, it must exercise the necessary and appropriate supervision over the entrusted person to ensure security control over the entrusted personal data. The handling operator must ensure that the entrusted person (e.g., the third-party service provider) has taken the same appropriate measures that the handling operator is required to take. The PPC Guidelines provide that “necessary and appropriate supervision” includes appropriately selecting the service provider, concluding the necessary contracts so that the security control measures based on Article 23 of the APPI (please see question 8.1) are observed by the service provider, and knowing the status of the handling of the personal data that was entrusted to the service provider.

9.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

There is no formality requirement, but the PPC Guidelines recommend that handling operators include the agreed security measures and the reporting requirement to enable the handling operators to know the status of the service provider’s handling of personal data. Under the financial sector guidelines, handling operators in the financial sector also need to include their right to supervise, audit and require reporting from the service provider, measures to prevent the leakage of personal data, the prohibition on the use of personal data for purposes other than agreed purposes, the prerequisites for subcontracting, and the responsibility of the service provider in the case of a leakage of personal data.

10 Marketing

10.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

Unsolicited marketing by email is regulated principally by the Anti-Spam Act. Pursuant to the Anti-Spam Act, marketing emails can be sent only to recipients who (a) “opted in” to receive them, (b) provided the sender with their email address in writing (for instance, by providing a business card), (c) have a business relationship with the sender, or (d) make their email address available on the internet for business purposes. In addition, the Anti-Spam Act requires the senders to allow the recipients to “opt out”. The Act on Specified Commercial Transactions also adopts the opt-in system for unsolicited marketing.

10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

The Anti-Spam Act applies not only to business-to-consumer marketing, but also to business-to-business marketing.

10.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

Unsolicited telephone marketing regarding certain items such as financial instruments (e.g., derivatives) is restricted under different regulations. There is no national opt-out register system.

10.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?

The Anti-Spam Act will apply to any entity, whether or not it has a presence in Japan, even if its marketing emails are sent from outside Japan, as long as the receiver is in Japan.

10.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

The MIC and the Consumer Affairs Agency are the authorities in charge of enforcing the Anti-Spam Act. There have been several enforcement cases initiated by those authorities, including a recent enforcement in March 2018.

10.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Purchasing a marketing list is not, in itself, illegal. However, the seller must obtain the consent of the principals, unless an exemption from the consent requirement applies. In addition, the seller must keep a record of certain information related to the provision of personal data for three years, and

the purchaser must be informed of the name and address of the seller, the name of the seller's representative and how the seller obtained the list, and must keep a record thereof for three years (APPI, Articles 29 and 30).

10.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

The maximum penalties under the Anti-Spam Act are one year of imprisonment or a fine of 1 million yen for an individual, and a fine of 30 million yen for the legal entity which employed that individual.

The maximum penalty for breaching the APPI is currently either imprisonment of up to one year or a fine of up to 1 million yen for individuals and 100 million yen for legal entities (APPI, Articles 178 and 184).

11 Cookies

11.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

If cookies, IP addresses and device IDs are collected at a web service or application knowing the identity of users (e.g., using user registration and log-in functions of the web service or application), they will be regulated as personal information. However, if they are collected without knowing the identity of users (e.g., user registration or log-in is not needed), they will not be regulated as personal information but may be regulated as person-related information. The collection and internal use of person-related information are not subject to any requirements under the APPI, but the provision of person-related information to third parties may be subject to a consent requirement under the APPI depending on how the data recipient will use the person-related information. If the recipient will receive the person-related information and link it to an identified user (e.g., a web service provider with a user registration feature receives cookies with certain attributes from third parties and links such cookies to its registered users), then it must obtain the consent of users and the data provider must ascertain that the consent has been obtained before the provision of person-related information.

Separately from the APPI, the Telecommunications Business Act regulates providers of (a) message exchange services, (b) social network services and other services to which users may post information, (c) search services, and (d) news sites or other services that distribute information to an unspecified audience, in the use of third-party cookies or other transmissions of information to third-party servers. Those providers must (i) provide a notification or disclosure about the use of cookies, (ii) obtain users' consent, or (iii) provide an opt-out to users.

11.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

The APPI distinguishes cookies based on how the cookies are used and not on the types. However, generally speaking, first-party cookies used by only one web service provider and not intended to be shared with third parties are usually not subject to the consent requirement, but third-party cookies intended to be shared with others may be subject to the

consent requirement if shared with a third party which plans to link the cookies to identified users.

Under the Telecommunications Business Act, (a) information originally transmitted by the service providers themselves (such as first-party cookies), and (b) information absolutely necessary to provide the service (such as OS, browser or language setting), are not subject to new requirements under the recent amendment of the Telecommunications Business Act.

11.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

Since the new regulations regarding cookies under the APPI took effect only in April 2022, there have been no enforcement cases yet.

The new regulations regarding cookies under the Telecommunications Business Act took effect in June 2023. As the regulations are very new, there have been no enforcement cases to date.

11.4 What are the maximum penalties for breaches of applicable cookie restrictions?

Under the APPI, an administrative fine of up to 100,000 yen may be imposed on a data recipient who falsely declares to the data provider that it has obtained the required consent.

Under the Telecommunications Business Act, as amended, a failure to comply with the requirements on transmissions of information to third parties is not directly punishable. However, the MIC may issue a remedial order and a breach of that order is punishable by a fine of up to 2 million yen.

12 Restrictions on International Data Transfers

12.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

The prior consent of the principals is required to transfer their personal data to a third party located in a foreign country (APPI, Article 28). However, the principals' prior consent to overseas transfers of their personal data is not necessary if (a) the foreign country is specified in the PPC Ordinance as having a data protection regime with a level of protection equivalent to that of Japan, or (b) the third-party recipient has a system of data protection which meets the standards to be prescribed by the PPC Ordinance.

As of 23 January 2019, the PPC has specified the EU and the UK as having a data protection regime with a level of protection equivalent to that of Japan by the PPC Ordinances (item (a) above). As of the same date, the European Commission also adopted the adequacy decision on Japan in accordance with Article 45 of the GDPR.

The PPC issued the Supplementary Rules for Personal Data, which have been transferred from the EU and the UK by adequacy decision. By the Supplementary Rules, the handling operators are subject to stricter regulations with regard to personal data.

The PPC Ordinance also provides that with respect to item (b), the third-party foreign recipient must either (i) provide assurance by appropriate and reasonable methodologies that it will treat the transferred personal information pursuant

to the spirit of the requirements for the handling of personal information under the APPI, or (ii) have been certified under a PPC-recognised international arrangement regarding its system of handling personal information (to date, the only PPC-recognised international arrangement is the APEC Cross-Border Privacy Rules System).

12.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

Prior to April 2022, many handling operators relied on the consent of data subjects. However, due to a new requirement for handling operators to provide information about the data protection regime of the jurisdiction to which the personal data will be transferred and the data protection measures taken by the data recipients before obtaining the consent of data subjects, more operators choose to rely on the third-party foreign recipient's assurance that it will treat the transferred personal data pursuant to the spirit of the requirements on the handling of personal information under the APPI (e.g., executing a data processing agreement to comply with the APPI). A handling operator that relies on such an assurance will need to regularly monitor the data protection of the data recipient and provide data subjects with information about the data protection of the data recipient if requested by data subjects.

12.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

There is no required notification or approval.

12.4 Do transfers of personal data to other jurisdictions require a transfer impact assessment? If conducting a transfer impact assessment is only mandatory in some circumstances, please identify those circumstances.

Article 23 of the APPI requires handling operators to take security measures in accordance with the PPC's guidelines. Section 10-7 of the PPC's Personal Information Protection Guidelines (General Rules) requires handling operators to understand the personal information protection regimes of any foreign jurisdiction where they handle personal information and to take necessary and appropriate measures considering such foreign regimes. In Japan, this required measure is not called a transfer impact assessment, but rather an external environment understanding.

12.5 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?

The PPC has not issued any guidance following the decision of the Court of Justice of the EU in *Schrems II*, probably because the adequacy decision on Japan would not be affected by the court decision.

12.6 What guidance (if any) has/have the data protection authority(ies) issued in relation to the use of standard contractual/model clauses as a mechanism for international data transfers?

The PPC has not issued any guidance regarding the use of standard contractual/model clauses issued by foreign authorities. From the Japanese regulatory perspective, the PPC's Personal Information Protection Guidelines (Rules for Data Transfer to Foreign Third Parties) should be considered.

13 Whistle-blower Hotlines

13.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

The Whistle-Blower Protection Act (*Koueki Tsuhosha Hogo Hou*) prohibits employers from dismissing whistle-blowers. Business operators employing more than 300 employees are required to, while business operators employing 300 or fewer employees are required to endeavour to, appoint a responsible person who will receive reports, investigate and take remedial measures, and take other measures to protect whistle-blowers.

13.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous reporting is generally permitted.

14 CCTV

14.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

There are no registration/notification requirements for the use of CCTV under the APPI. However, the PPC clarified the requirements applicable to the use of CCTV in its Q&A published in May 2023. If the use of CCTV is apparent to visitors and is used solely for the purpose of crime prevention (and not for identifying a person, marketing or other purposes), notification to visitors is not strictly required but only recommended. On the other hand, if CCTV is used for identifying a person (e.g., matching an identified person to those on a black list), the purposes of crime prevention and such identification must be notified or announced to visitors, and the PPC also recommends that additional information such as contact information and access to a website URL or a QR code for further information be posted near the CCTV.

14.2 Are there limits on the purposes for which CCTV data may be used?

In March 2023, the PPC issued a report regarding the use of CCTV to identify persons. Since such use of CCTV may cause an invasion of privacy and discrimination, the report recommends that users of CCTV consider whether that use of CCTV is

absolutely necessary for crime prevention and assess whether the necessity outweighs the risks of invasion of privacy and discrimination.

15 Employee Monitoring

15.1 What types of employee monitoring are permitted (if any), and in what circumstances?

The employer has the right to monitor workplace communications in relation to work. However, a privacy issue may arise regarding private communications in the workplace. Thus, it is recommended that employers establish internal rules prohibiting the use of company PCs and email addresses for private use, and disclosing the possibility of monitoring those devices and data.

15.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Please see question 15.3.

15.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

There are no statutory or special requirements for notification to or consultation with trade unions/employee representatives regarding employee monitoring. However, if an employer sets up internal rules on employee monitoring, these rules will be considered company work rules and would require prior notification to or consultation with the majority union or employee representative.

15.4 Are employers entitled to process information on an employee's attendance in office (e.g., to monitor compliance with any internal return-to-office policies)?

If an employer notifies the purpose of use to the employees before collecting their attendance status, then it may collect the status and use it for the notified purpose.

16 Data Security and Data Breach

16.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

A handling operator is obligated to take necessary and proper measures to prevent leakage, loss or damage, and for other security control, of personal data (APPI, Article 23). Further, the handling operator is required to exercise necessary and appropriate supervision over its employees and service providers to ensure the security control of personal data (*id.* Articles 24 and 25). There is no concept of controllers or processors under the APPI (please see question 2.1).

16.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Handling operators are required to report material data breaches (please see question 2.1) to personal data to the PPC.

Further, under the financial sector guidelines (please see question 1.3), a handling operator in the financial sector must also report non-material data breaches to the Financial Services Agency.

16.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Handling operators are required to report material data breaches relating to personal data to the affected principals unless it is difficult to make that report and an alternative measure is taken. They are also required to report material data breaches to the PPC. Under the current regulations, a preliminary report must be filed with the PPC without delay (suggested to mean three to five days under the PPC guidelines) and a final report must be filed with the PPC within 30 days (or 60 days with regard to a data breach potentially caused by a malicious act) after the data breach becomes known to the handling operators. The PPC proposes to grant an exemption from the filing of preliminary reports where approved by an Authorised Entity.

16.4 What are the maximum penalties for personal data security breaches?

If a handling operator provides or misuses a personal information database for the purpose of unlawful gains, it may be subject to imprisonment of up to one year, or a fine of up to 500,000 yen (*id.* Article 179). If the breach is committed by a person who is employed by an entity, such entity will be subject to a fine of up to 100 million yen (*id.* Article 184).

17 Enforcement and Sanctions

17.1 Describe the enforcement powers of the data protection authority(ies).

- (a) **Investigative powers:** The PPC may require a handling operator to report or submit materials regarding its handling of personal information, enter offices or other places to conduct an investigation, make inquiries and check records or other documents (APPI, Article 146), and require, for the protection of personal information, an Authorised Entity to report regarding its activities (*id.* Article 153).
- (b) **Corrective powers:** The PPC may render guidance or advice to a handling operator (*id.* Article 147), recommend a handling operator to cease the violation, take necessary measures to correct the violation and other necessary

measures (*id.* Article 148) and order an Authorised Entity for the protection of personal information to take necessary measures (*id.* Article 154).

- (c) **Authorisation and advisory powers:** The PPC does not have a general authorisation or advisory power, but has the authority to grant authorisation to applicant entities to become Authorised Entities.
- (d) **Imposition of administrative fines for infringements of specified GDPR provisions:** The PPC will enforce their investigating or corrective powers under the APPI, but do not have the authority to enforce GDPR provisions.
- (e) **Non-compliance with a data protection authority:** If an order issued by the PPC is breached, an individual may be subject to imprisonment of up to one year, or a fine of up to 1 million yen (*id.* Article 178), and the legal entity employing the individual will also be subject to a fine of up to 100 million yen (*id.* Article 184). The PPC proposes to introduce an administrative monetary penalty for breaches of the APPI.

17.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

In relation to the PPC's powers stated in question 17.1 above, the PPC would have the power to issue an order to ban a particular processing activity without the need for a court order.

17.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

In general, the PPC renders guidance in the case of a relatively less important violation, and a recommendation in the case of a more important violation. The PPC issued one order to a business entity to cease the provision of personal data.

17.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

Partly because the PPC's enforcement power was limited to rendering guidance, advice or recommendations to the handling operators outside Japan prior to April 2022, there have been limited cases in which the PPC exercised its powers against handling operators outside Japan. Following April 2022, the PPC was granted the authority to issue orders to handling operators outside Japan to take remedial measures.

18 E-discovery/Disclosure to Foreign Law Enforcement Agencies

18.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Under the APPI, the general rule is that the handling operator cannot provide personal data to any "third party" without obtaining the prior consent of the principal, except in specified cases (Article 27, paragraph 1). These specified cases are cases where the provision of personal data is:

- (a) required by laws and regulations;

- (b) necessary to protect the life, body or property of a person and it is difficult to obtain the consent of the principal;
- (c) necessary to improve public health and promote the sound nurturing of the young and it is difficult to obtain the consent of the principal;
- (d) necessary for governmental bodies to perform their business, and getting the consent of the principal will likely impede the proper performance of such business;
- (e) where the handling operator is an academic research institute, necessary for publishing or teaching research results;
- (f) where the handling operator is an academic research institute, necessary to provide personal data to a third party for joint research; or
- (g) where the third-party recipient is an academic research institute, necessary for academic research purposes.

It is understood that "governmental bodies" referenced in (d) above would be bodies of the Japanese government and not of other countries, and "laws" referenced in (a) above would not include foreign laws. If the handling operator were compelled to disclose personal information of Japanese individuals in accordance with a foreign law or by an action of a foreign governmental institution, the handling operator may be able to disclose the personal data in accordance with (b) above; however, to avoid any risk in this regard, it is practical to obtain the prior consent of the data subjects before transferring data in response to requests from foreign law enforcement agencies.

18.2 What guidance has/have the data protection authority(ies) issued on disclosure of personal data to foreign law enforcement or governmental bodies?

There is no specific guidance from the PPC regarding the response to requests for disclosure from foreign law enforcement or governmental bodies.

19 Artificial Intelligence

19.1 Are there any limitations on automated decision-making involving the processing of personal data using artificial intelligence?

There have been no laws to specifically regulate artificial intelligence ("AI") in the context of personal data processing, but a new legislation titled the Act on Promotion of Research, Development, and Utilization of AI-Related Technologies was passed by the Diet in May 2025. The Act clarifies that appropriate measures are necessary to prevent criminal activities, leakage of personal information, infringement of copyrights, and other harms to the tranquility of citizens' lives and their rights and interests in the research, development, and utilisation of AI-related technologies. There is no sanction against breaches, but the national government is mandated to provide advice, guidance and information to, and take other necessary measures against, business operators using AI-related technologies.

19.2 What guidance (if any) has/have the data protection authority(ies) issued in relation to the processing of personal data in connection with artificial intelligence?

The PPC issued a guidance regarding use of generative AI in June 2023. The guidance requires generative AI users to (a)

carefully consider whether the input of personal data to generative AI is within the notified purposes of the data collection, and (b) carefully ascertain that the input of personal data as a prompt to generative AI is used only to process the prompt and not for machine learning, unless users' consent is obtained. The guidance also requires AI developers not to (i) collect sensitive personal data for machine learning, and (ii) use sensitive personal data inputted as a prompt without a justifiable reason.

20 Trends and Developments

20.1 In your opinion, what enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.

As per questions 1.1 and 1.4, the PPC, as an independent regulatory body, has the authority to enforce the APPI. The enforcement cases brought by the PPC regarding the APPI in FY 2024 (April 2024 to March 2025) were: 67 cases where the PPC required handling operators to report or submit materials regarding their handling of personal information; and 395 cases where the PPC rendered guidance or advice.

20.2 In your opinion, what "hot topics" are currently a focus for the data protection regulator?

There is a legal mandate to update the APPI every three years. In the discussions on the next update, the PPC proposed in March 2025 the following pro-business deregulations:

- Allowing use of personal data, including sensitive personal data, without consent where absolutely necessary or apparently not infringing data subjects' rights.
 - Allowing use of personal data to protect life or public health without consent where there is a justifiable reason not to obtain consent.
 - Allowing hospitals to use personal data for research.
 - Exempting data breach notification to data subjects where data subjects' rights are unlikely to be infringed.
 - Exempting preliminary data breach notification to the PPC where approved by an Authorised Entity.
- At the same time, the PPC proposes to strengthen regulations as follows:
- Requiring guardians' consent to process the personal data of a minor under the age of 16.
 - Introducing prohibition of unjustifiable or fraudulent collection of person-related information not regulated as personal data, but which can be exploited for fraud.
 - Requiring extended disclosure for use of face recognition data.
 - Introducing a due diligence obligation where personal data is provided to third parties in an opt-out scheme.
 - Strengthening the PPC's enforcement capacity such as issuing injunction orders, disclosure orders, and orders to request third-party service providers to cease provision of services to illegal actors.
 - Introducing third party personal data provision as a crime.
 - Introducing administrative monetary sanctions.
 - Introducing collective injunction and redress schemes.
- Allowing use of personal data, including sensitive personal data, without consent for statistical processing, including AI developments.



Hiromi Hayashi is a partner at Mori Hamada & Matsumoto, which she joined in 2001. She specialises in communications law and regulation and authored the Japanese section of *Telecommunication in Asia* in 2005. Her other areas of practice are international and domestic transactions, takeover bids and corporate restructuring. Hiromi was admitted to the Bar in 2001 in Japan and in 2007 in New York. She worked at Mizuho Corporate Bank from 1989 to 1994 and at Davis Polk & Wardwell in New York from 2006 to 2007.

Mori Hamada & Matsumoto
Marunouchi Park Building, 2-6-1
Marunouchi Chiyoda-ku
Tokyo 100-8222
Japan

Tel: +81 3 5220 1811
Email: hiromi.hayashi@morihamada.com
LinkedIn: www.linkedin.com/in/hiromi-hayashi-25676384



Masaki Yukawa is a counsel at Mori Hamada & Matsumoto, which he joined in 2009. He advises on Japanese data protection issues for domestic and international technology companies, e-commerce companies and financial institutions. He was admitted to the Bar in 2009 in Japan and in 2016 in California. He is an Information Security Specialist registered with the Information-technology Promotion Agency of Japan.

Mori Hamada & Matsumoto
Marunouchi Park Building, 2-6-1
Marunouchi Chiyoda-ku
Tokyo 100-8222
Japan

Tel: +81 3 6266 8764
Email: masaki.yukawa@morihamada.com
LinkedIn: www.linkedin.com/in/masakiyukawa

Mori Hamada & Matsumoto is a premier international law firm headquartered in Japan. We provide full-service legal support for diverse business activities worldwide. We have the largest and most extensive network in Japan as well as strong global presence, enabling us to offer seamless cross-border solutions.

We deliver comprehensive and integrated legal services across all areas of business law, using innovative technology to enhance efficiency and quality. We understand our clients' specific needs and objectives, and we tailor our solutions to ensure optimal outcomes.

Our reputation and expertise are built on decades of practical experience and a proven track record. Our mission is to create value for our clients, foster professional growth for our people, and make a positive impact on the community.

www.morihamada.com



Mexico

Mexico



Abraham Diaz



Gustavo Alcocer



Carla Huitron

OLIVARES

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The legal framework for data protection is found in Articles 6 and 16 of the Mexican Constitution, as well as in the new Federal Law for the Protection of Personal Data Held by Private Parties, published on March 20, 2025, and its Regulations, published in December 2011 (hereinafter the “FLPPDHPP”).

1.2 Is there any other general legislation that impacts data protection?

Yes: the New General Law for the Protection of Personal Data in the Possession of Obligated Subjects, also published on March 20, 2025, which regulates the processing of personal information (“PI”) in the possession of any Federal, State or local governmental authorities (“the Law”); the Privacy Notice Rules, published in January 2013; the Binding Self-Regulation Parameters, also published in January 2013; and the General Guidelines for the Protection of Personal Data for the public sector (Federal, State or local authorities). It is worth mentioning that Mexican data protection laws and general legislation follow international correlative laws, directives and statutes, and thus have similar principles, regulatory scope and provisions. Moreover, there are other laws such as: the Criminal Code; the Law for the Regulation of Credit Information Companies; the Law for Regulating Financing Technology Institutions; provisions set forth in the Copyright Law and the Federal Law for Consumer Protection; and some specific provisions set forth in the Civil Code and the Commerce Code, which are also related to data protection.

1.3 Is there any sector-specific legislation that impacts data protection?

Mexican data protection legislation is not based on sectoral laws. The Law, as described above, is a general law that regulates the collection and processing of any PI by any private entity acting as a Controller or Processor, which impacts any sector that is involved in any sort of personal data collection or processing.

1.4 What authority(ies) are responsible for data protection?

Up to March 20, 2025, the National Institute of Transparency, Access to Information and Personal Data Protection (“INAI”) was the authority responsible for overseeing the Law.

As of March 21, 2025, the authority responsible for overseeing the Law is the Ministry of Anti-Corruption and Good Government (“Ministry of ACGG”), which main purpose will be the disclosure of governmental activities, budgets and overall public information, as well as the protection of personal data and the individuals’ right to privacy. The Ministry of ACGG has the authority to: conduct investigations; review and sanction data protection Controllers; and authorise, oversee and revoke certifying entities.

The Ministry is responsible for informing and educating on the obligations regarding the protection of personal data between national and international corporations with commercial activities in the Mexican territory.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **“Personal Data”**
Any information concerning an individual that may be identified or identifiable. It is considered that a person is identifiable when their identity may be determined directly or indirectly by any information.
- **“Processing”**
Any operation or set of operations done by manual or automated procedures applied to personal data, related to obtaining, using, recording, organising, preserving, elaborating, communicating, disseminating, storing, possessing, accessing, handling, using, disclosing, transferring or disposing of personal data.
- **“Controller”**
Private individuals or legal entities that carry out the processing of personal data.
- **“Processor”**
The individual or legal entity that, solely or jointly with another, processes personal data on behalf of the Controller.
- **“Data Subject”**
Any identified or identifiable natural person.

■ **“Sensitive Personal Data”/“Special Categories of Personal Data”**

Any personal data that may affect the most intimate sphere of an individual, or that which, if misused, may lead to discrimination or carry a serious risk to the individual. By way of example, but not limiting, sensitive personal data are considered those that may reveal information such as ethnic or racial origin, a present or future medical condition, genetic information, religious, philosophical and moral beliefs, union affiliation, political opinions and sexual preference.

Other than the “sensitive personal data definition” there are no special categories of personal data in our law.

■ **“Data Breach”**

Data breach means any security breach that, if occurring in any phase of the data collection, storage or use, may affect in a significant manner the patrimonial or moral rights of individuals.

■ **“Pseudonymous Data”**

Such data that is processed in such a way that it can no longer be attributed to a specific data subject, without the use of additional information.

3 Territorial and Material Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

Mexican data protection law is not limited to PI Controllers established or operating in Mexican territory. Although the Law does not provide a specific reach or scope of its applicability, the Regulations to the Law do. In this regard, such regulations (and, therefore, the Law), in addition to being applicable to companies established or operating under Mexican law (whether or not located in Mexican territory) apply to companies not established under Mexican law that are subject to Mexican legislation derived from the execution of a contract or under the terms of international law.

Additionally, Mexican regulations on data protection apply to: company establishments located in the Mexican territory; persons or entities not established in the Mexican territory but using means located in such territory, unless such means are used merely for transition purposes that do not imply a processing or handling of personal data; and when the Controller is not established in the Mexican territory but the person designated as the party in charge of the control and management of its personal data (a service provider) is.

In the case of individuals, the establishment will mean the location of the main place of business or location customarily used to perform their activities or their home.

3.2 Do the data protection laws in your jurisdiction carve out certain processing activities from their material scope?

Mexican Data Privacy Law does not carve out any processing activities from the material scope. Our Law only indicates that the Controller should be responsible for processing personal and/or sensitive data in accordance with the principles set forth in the Law and international treaties, regardless of the processing activity or material scope.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

■ **Transparency**

This principle is not defined in the Law; however, the Law makes it clear that personal data can in no way be collected, stored or used through deceitful or fraudulent means.

■ **Lawful basis for processing**

The Controller is responsible for processing personal and/or sensitive data in accordance with the principles set forth in the Law and international treaties.

■ **Purpose limitation**

Personal data shall only be collected and processed in compliance with the purpose or purposes set forth in the Privacy Notice. Moreover, the purpose of the Privacy Notice must be certain, which is achieved by establishing the purpose for which the personal data will be collected and processed in a clear, objective manner, not leaving any room for confusion.

■ **Data minimisation**

The Controller will be responsible and shall endeavour to make reasonable efforts so that the personal data processed are the minimum necessary according to the purpose that originated the collection of PI.

■ **Proportionality**

Controllers can only collect personal data that are necessary, appropriate and relevant for the purpose(s) of their collection.

■ **Retention**

This translates into the obligation of the Controller to retain personal data only for the period of time necessary for complying with the purpose(s) for which the data were collected, with the obligation to block, cancel and suppress the personal data afterwards.

■ **Accuracy**

This principle refers to ensuring that the processed personal data is correct and updated and is strictly related to the following “Quality” principle as described below, which includes accuracy.

■ **Responsibility**

The Controller must safeguard and be accountable for any PI under its custody, or any PI that it has shared with any vendor, either in Mexico or abroad. In order to comply with this principle, the Controller must make use of any of the best international practices, corporate policies, self-regulatory schemes or any other suitable mechanism to this effect.

■ **Quality**

This principle is accomplished when the personal data processed are accurate, complete, pertinent, correct and updated as required, in order to comply with the purpose for which the personal data will be collected.

■ **Consent**

The Controller must obtain the consent of the data subject at the moment in which PI is being collected and must keep evidence of the consent.

■ **Loyalty**

This consists of the obligation of the Controller to process any PI collected favouring the protection of the interests of the data subject and the reasonable expectation of privacy.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to (copies of) data/information about processing**
Data subjects have the right to access their personal data held by the Controller at any time they request.
- **Right to rectification of errors**
Data subjects have the right to request the rectification of any of their personal data, held by a Controller, which turns out to be inaccurate, incomplete or out of date.
- **Right to deletion/right to be forgotten**
Data subjects have the right to request the cancellation of their personal data. The cancellation of personal data will result in a blocking period, after which the suppression of the data will take place. Notwithstanding the foregoing, the Controller may keep such personal data exclusively for the purposes of the responsibilities regarding their treatment. Likewise, the Law establishes some cases where the Controller is not obliged to cancel or delete the personal data.
- **Right to object to processing**
Data subjects have the right to object to the processing of their personal data due to a legitimate reason.
- **Right to restrict processing**
Data subjects have the right to restrict the processing of their personal data due to a legitimate reason.
- **Right to data portability**
Data subjects have the right to obtain, from the subject concerned, a copy of their processed data, which allows the data subject to continue using their PI.
- **Right to withdraw consent**
At any time, the data subject may withdraw their consent for the treatment of their personal data. The Controller must establish simple and free mechanisms that allow the data subjects to withdraw their consent at least by the same means by which they granted it.
- **Right to object to marketing**
In addition to the general rights described above, data subjects have the right to oppose the use of their personal data for marketing or advertising purposes.
- **Right protecting against solely automated decision-making and profiling**
Data subjects have the right to oppose to the treatment of their data, at any time, by any mechanism, including automated decision-making and profiling.
- **Right to complain to the relevant data protection authority(ies)**
Data subjects are entitled to submit a claim before the Ministry of ACGG. The claim must be filed in writing and must clearly state the provisions of the Law that are deemed infringed; also, it must be submitted within the 15 days following the date on which the response to the data subject has been communicated by the Controller.
- **Right to a verification procedure**
Data subjects have the right to request a verification procedure before the Ministry of ACGG, by which the authorities will check the Controller's compliance with all the provisions set forth in the Law, or any other applicable regulations.

5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

The only person that might seek remedies for data protection infringements are the data owners themselves, or in its case, their legal representatives. The Law does not contemplate collective redress.

6 Children's Personal Data

6.1 What additional obligations apply to the processing of children's personal data?

Children's legal guardians' consent must be always given when processing children's personal data. This applies to any individual younger than 18 years of age.

7 Registration Formalities and Prior Approval

7.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

No, there is not.

7.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

This is not applicable.

7.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

This is not applicable.

7.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

This is not applicable.

7.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

This is not applicable.

7.6 What are the sanctions for failure to register/notify where required?

This is not applicable.

7.7 What is the fee per registration/notification (if applicable)?

This is not applicable.

7.8 How frequently must registrations/notifications be renewed (if applicable)?

This is not applicable.

7.9 Is any prior approval required from the data protection regulator?

This is not applicable.

7.10 Can the registration/notification be completed online?

This is not applicable.

7.11 Is there a publicly available list of completed registrations/notifications?

This is not applicable.

7.12 How long does a typical registration/notification process take?

This is not applicable.

8 Appointment of a Data Protection Officer

8.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The appointment of a Data Protection Officer (person or department) by the Controller is mandatory.

8.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

Failure to appoint a Data Protection Officer (person or department) is not expressly catalogued as an infringement in the Law. However, Section XIX of Article 58 of the FLPPDHPP contains a “catch all” provision that considers any failure to comply with the obligations set forth in the Law to be an infringement. Therefore, failure to appoint a Data Protection Officer must be deemed an administrative infringement. Nevertheless, there is no express sanction in the law for the infringements referred to in Section XIX above.

8.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

No, they are not.

8.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

Yes, it can.

8.5 Please describe any specific qualifications for the Data Protection Officer required by law.

There are no statutory requirements. Notwithstanding the foregoing, it is recommended to appoint a person, team or department with at least the following qualifications: (i) data privacy expertise (certification desired); and (ii) enough authority and resources to advocate and implement measures in order to protect the personal data within the company.

8.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

The responsibilities of a Data Protection Officer required by law are to: (i) process all claims related to the enforcement of ARCO rights; and (ii) foster and enhance the protection of personal data inside the company.

8.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

No, there is no statutory obligation to register or notify the appointment of a Data Protection Officer to any authority.

8.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

It is necessary to mention in the Privacy Notice the name and domicile (contact information) of the person or department that will be responsible for the collection, use and storage of the personal data.

9 Appointment of Processors

9.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes, the relationship between the business and the Processor must be established by means of contractual clauses or other legal instruments determined by the business; and it is necessary to prove the existence, scope and content of the relationship.

9.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The agreement must be in writing and signed by both parties. The agreement must contain at least the following obligations on the Processor: (i) to treat personal data according to the instructions of the business; (ii) to treat personal data for the purposes instructed by the business; (iii) to implement security measures in accordance with the Law, and other

applicable provisions; (iv) to keep confidentiality regarding the personal data processed; (v) to delete all PI processed once the legal relationship with the business is over, or when the instructions of the business have been fulfilled, provided that there is no legal provision that requires the preservation of the personal data; and (vi) to refrain from transferring PI unless the business determines so, or when it is required by a competent authority. It is worth mentioning that agreements between the business and the Processor in relation to the treatment of personal data must be in accordance with the corresponding Privacy Notice.

10 Marketing

10.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

Mexico does not have any specific regulations dealing with unsolicited text messages or spam emails, but the Federal Bureau for Consumer Protection operates a call-blocking registry, covering both landlines and mobile phone numbers, which gives suppliers 30 days to make marketing calls, send marketing messages and to stop disturbing the consumer at his/her registered address, electronic address, or by any other means. Likewise, all the marketing purposes must be specified clearly in the Privacy Notice.

10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

Please refer to question 10.1 above.

10.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

Please refer to question 10.1 above.

10.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Please refer to question 10.1 above.

10.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

Issues regarding marketing restrictions are regularly addressed by the Federal Bureau for Consumer Protection.

10.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Since Mexican law expressly provides that the collecting or processing of any PI must be through lawful means, the purchasing of marketing lists, including any PI not collected

in accordance with Mexican law, would not be deemed legal. If the marketing list includes only business contact information or publicly available information, then it can be used, and it is always recommended to provide recipients of emails sent for marketing purposes with a mechanism that allows an easy opt-out from the marketing service.

10.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

According to the Federal Consumer Protection Law, the maximum penalties for marketing breaches may reach the amount of MXN\$2.2 million (approximately US\$109,000 at an exchange rate of MXN\$20.3 per dollar).

11 Cookies

11.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

The Guidelines for drawing up the Privacy Notice require that individuals be informed as to any technology that allows the automatic collection of PI simultaneously with the first contact with the individuals; data owners to request consent from individuals through an opt-in mechanism; and individuals to be informed as to how to deactivate said technology, unless said technology is required for technical reasons.

11.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

No, they do not.

11.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

No, they have not.

11.4 What are the maximum penalties for breaches of applicable cookie restrictions?

Although there is not any express infringement regulated in the Law in connection with the use of cookies, their use in contravention of the Guidelines mentioned above would translate to an illicit collecting of PI, which would be sanctioned with a fine of up to US\$1.9 million, and if the infringement persists, an additional fine of up to US\$1.9 million may be imposed.

12 Restrictions on International Data Transfers

12.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

If the Controller wishes to transfer any PI to any third parties, either domestic or foreign, it needs to obtain the informed consent of data subjects for the said data transfer, in advance, through the corresponding Privacy Notice. There are some

cases where third parties do not require the consent of the data subject for the transfer of PI. According to Article 36 of the Law, consent will not be necessary only in the following cases:

- (i) when expressly permitted by the Law;
- (ii) when PI is available in publicly accessible sources;
- (iii) when personal data has been dissociated;
- (iv) when the collection of personal data is needed for compliance with obligations derived from a legal relationship between the data subject and the data owner;
- (v) when there is an emergency situation that jeopardises the person or the commodities of the data subject; and
- (vi) when the collection of PI is indispensable for medical attention and/or diagnosis, rendering sanitary assistance, and medical treatment or sanitary services, provided that the data subject is not in a condition to give consent, and provided that the data collection is performed by a person subject to legal professional privilege.

12.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

As stated above, according to Article 35 of the Law, if a Controller wishes to transfer any PI to third parties, either domestic or foreign, it must obtain consent from the data subject in advance, through a Privacy Notice. When the transfer is performed, the vendor or third party will be obliged on exactly the same terms as the Controller, by means of an agreement that must be executed in writing.

12.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

There is no registration/notification requirement set forth in the Law for data transfers.

12.4 Do transfers of personal data to other jurisdictions require a transfer impact assessment? If conducting a transfer impact assessment is only mandatory in some circumstances, please identify those circumstances.

Conducting a transfer impact assessment is not mandatory under our Law, for transfer of personal data to other jurisdictions.

12.5 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?

There has been no guidance from the Mexican DPA following the decision of the Court of Justice of the EU in *Schrems II* (Case-311/18).

12.6 What guidance (if any) has/have the data protection authority(ies) issued in relation to the use of standard contractual/model clauses as a mechanism for international data transfers?

There has been no guidance in relation to the use of standard contractual/model clauses as a mechanism for international data transfer, directly issued by the Mexican DPA. However, as part of the Ibero-American Data Protection Network, the Mexican DPA contributed in the elaboration of the “Implementation Guide on Model Contractual Clauses for the International Transfer of Personal Information”, which can be consulted at: <https://www.redipd.org/sites/default/files/2023-02/guia-implementacion-clausulas-contractuales-modelo-tidp-es.pdf> (available only in Spanish language).

This is not an official document and does not constitute any regulation. The principles discussed in this guide are still to be enacted in Mexican regulations and in the Mexican DPA’s resolutions.

13 Whistle-blower Hotlines

13.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

Whistle-blower hotlines can be put into operation, but the Law is silent as to any restrictions on the personal data that may be processed through them.

13.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous and non-anonymous reporting is permitted.

14 CCTV

14.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

There is no registration or notification requirement for the use of CCTV.

14.2 Are there limits on the purposes for which CCTV data may be used?

The Law is silent as to the limits on the purposes for which CCTV data may be used.

15 Employee Monitoring

15.1 What types of employee monitoring are permitted (if any), and in what circumstances?

In January 2021, there was an amendment to the Mexican Federal Labor Law, introducing the regulation of “telework”,

thus establishing the right of employers to monitor employees' activities working under this modality, and the obligation of employees to use the technology provided by employers in order to monitor the activities carried out under the modality of telework.

The monitoring of the employee is limited to the activities carried out under the modality of telework, and this amendment also recognises the right of employees to "disconnect", whenever they are not performing their work, in order to respect their privacy.

This amendment only established a general legal framework that will have to be detailed soon.

The general rules set forth by this amendment will also have to be interpreted by the Mexican Courts on a case-by-case basis, in order to generate jurisprudence in this regard.

15.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

A written agreement will have to be executed between the employer and employees working under the modality of telework, and in said agreement the consent to be monitored during working hours will have to be collected.

Also, since the collection, storage and use of any audio or video material featuring the voice and image of any individual within the workplace may be deemed a collection of PI, employers are required to give employees notice as to the use of video surveillance technology at workplaces.

In the past, the data protection authority drew up a short model Privacy Notice to be used by any individual or company introducing video surveillance technology on their premises.

Said summary Privacy Notice must be visible at the entrance to monitored spaces and must inform individuals of the purpose of the surveillance and the treatment of the collected information.

15.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

Currently, it is not mandatory to consult or notify employees' representatives at works councils/trade unions. However, in light of the above-mentioned amendment, it may change in the near future when negotiating collective labour agreements for employees working under the modality of telework.

15.4 Are employers entitled to process information on an employee's attendance in office (e.g., to monitor compliance with any internal return-to-office policies)?

Yes, as long as an employment agreement exists that includes a data protection clause, by which an employer is entitled to monitor employees' attendance in office as a result of its internal policies and such policies are duly presented to employees.

16 Data Security and Data Breach

16.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Article 18 of the FLPPDHPP requires every Controller to implement and maintain administrative, technical and physical

security measures, which protect the collected and stored PI from any loss, alteration, destruction or any unauthorised access and use.

Said measures cannot be lesser than those used by the data owner to protect its own information. For their implementation, the data Controller must consider the existing risk and the possible consequences for the data subjects, the sensitivity of the data, and technological developments. Therefore, security measures may vary from industry to industry, and from company to company.

16.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

There is no legal requirement to report data breaches to the Ministry of ACGG, and so far, there are no guidelines for voluntary breach reporting to the authority.

16.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Mexican law sets forth that if any phase of collection, storage or use of data "may in any way affect in a significant manner the patrimonial or moral rights of individuals", data owners must immediately notify individuals about this situation.

However, so far there is no further explanation in the law or in the jurisprudence as to what is to be deemed a significant effect on the patrimonial or moral rights of data subjects.

Likewise, Article 64 of the Regulations of the Law requires data owners to notify individuals, without any delay, as to any breach that significantly affects their moral or patrimonial rights, as soon as the data owner confirms that a breach has occurred, and when the data owner has taken any actions towards starting an exhaustive process to determine the magnitude of the breach.

In said notification, data owners must state at least:

- the nature of the incident;
- the compromised PI;
- recommendations for the data subjects to protect their interests;
- the corrective measures immediately implemented by the data owner; and
- the means of obtaining more information regarding the breach.

16.4 What are the maximum penalties for personal data security breaches?

If the personal data authority (Ministry of ACGG) determines that a personal data breach is attributable to a Controller or Processor, a fine up to US\$1.7 million may be imposed depending on the breach.

Likewise, a prison sentence ranging from three months to three years shall be imposed on any individual who, being authorised to handle personal data, causes a security breach

in the databases under their custody with the intent of obtaining financial gain.

If the personal data security breach refers to sensitive personal data, then these amounts may be duplicated.

17 Enforcement and Sanctions

17.1 Describe the enforcement powers of the data protection authority(ies).

- (a) **Investigative powers:** Verification proceeding: the Ministry is entitled to conduct inspections *ex officio* at any company, in order to determine its compliance with the legislation on PI.
- (b) **Corrective powers:** The Ministry is entitled to declare administrative infringements in order to enforce the ARCO rights of any individual, for omitting in the Privacy Notice any or all of the elements established in the Law, collecting or transferring personal data without the express consent of the holder, for obstructing the authority's acts of verification, and violating the security of databases, programs or equipment, when it is attributable to the responsible party, among others.
As of March 21, 2025, any resolutions issued by the new Ministry of ACGG may be challenged through an *amparo* lawsuit before specialised courts in the field.
- (c) **Authorisation and advisory powers:** The Ministry is entitled to develop, promote and disseminate analyses, studies and research on the protection of personal data held by private parties and to provide training to regulated entities. It may also provide technical support to those responsible, upon request, for compliance with the obligations established in the Law.
- (d) **Imposition of administrative fines for infringements of specified legal provisions:** The Ministry is entitled to declare administrative infringements and impose administrative fines for non-compliance with any of the principles or provisions of the Law.
As of March 21, 2025, any resolutions issued by the new Ministry of ACGG may be challenged through an *amparo* lawsuit before specialised courts in the field.
- (e) **Non-compliance with a data protection authority:** The Ministry is entitled to issue the criteria and recommendations, in accordance with the applicable provisions of this Law, for the purposes of its enforceability and operation.

17.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

This authority is not expressly designated in the Law as the Ministry of ACGG. However, considering that the Law recognises the Ministry of ACGG as the specialised authority in charge of the protection of PI in Mexico, the Ministry should be deemed as having the authority to ban a particular processing activity. However, if contested by any third party, any ban issued by the Ministry should be validated by the Mexican Federal Administrative Courts.

As mentioned above, as of March 21, 2025, any resolutions issued by the new Ministry of ACGG may be challenged through an *amparo* lawsuit before specialised courts in the field.

17.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

There are no recent cases or precedents illustrating the data protection authority's approach.

17.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

At the time of writing, there is no precedent for the data protection authority having exercised its powers against businesses established in other jurisdictions.

18 E-discovery/Disclosure to Foreign Law Enforcement Agencies

18.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Any e-discovery requests or requests for disclosure from foreign law enforcement agencies must be validated by Mexican Courts for them to be validly enforced in Mexico. If any order or request from any foreign law enforcement agency is not validated through a Mexican Court, a company may refuse to comply with it.

18.2 What guidance has/have the data protection authority(ies) issued on disclosure of personal data to foreign law enforcement or governmental bodies?

No guidance has been issued by our data protection authority on disclosure of personal data to foreign law enforcement or governmental bodies.

19 Artificial Intelligence

19.1 Are there any limitations on automated decision-making involving the processing of personal data using artificial intelligence?

So far, no law in Mexico regulates the use of artificial intelligence ("AI"), and no modifications to the FLPPDHPP have been made to include the processing of personal data using AI; however, automated decision-making (such as the use of cookies) is regulated in the Law and its regulations and guidelines (please refer to section 11 above). Hence, said provision can be construed to include any AI automated decision-making.

19.2 What guidance (if any) has/have the data protection authority(ies) issued in relation to the processing of personal data in connection with artificial intelligence?

This is not applicable; please refer to our previous answer.

20 Trends and Developments

20.1 In your opinion, what enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.

While Mexico's INAI was officially extinguished in March 2025, prior to that and over the last 12 months, there were several important enforcement trends and signals in data privacy that are worth noting:

- Data processing practices of online retailers and digital advertisers came under scrutiny, especially regarding unsolicited marketing messages (email/SMS) and inadequate consent.
- Companies received guidance and sanctions for vague, incomplete or overly generic privacy notices.
- INAI became stricter as to the evidence submitted by data controllers, the consent obtained and the measures adopted to protect any collected PI.

The most recent notable case handled by INAI was an investigation into the Mexican Football Federation ("FMF") in February 2025. INAI initiated a sanctioning procedure against the FMF concerning the use of the Fan ID application, which collects personal and biometric data from fans.

The key points are as follows:

- **Data collection:** The Fan ID app was implemented to identify fans involved in inappropriate behaviour during matches.
- **Third-party involvement:** Data was collected through Incode Technologies.
- **INAI's determination:** Despite the involvement of Incode, INAI held FMF responsible for data handling practices.

The investigation's results could impact Mexico's role as a host for the 2026 World Cup.

20.2 In your opinion, what "hot topics" are currently a focus for the data protection regulator?

- (1) In accordance with the recent constitutional reform dated November 28, 2024, the extinction of seven autonomous agencies was decreed, including the INAI.

On March 20, 2025, a Decree was published in the Official Gazette, enacting the new FLPPDHPP, as well as a new General Law on the Protection of Personal Data Held by Obligated Subjects.

These two laws came into effect as of March 21, 2025, formalising the extinction of the INAI. It appears that the personal data protection framework – both for data held by private entities and by public entities of the Mexican Government – remains unchanged. There are no modifications to the rights of data subjects or to the obligations of those who process personal data. Likewise, no changes have been observed in the legal framework for transparency and access to information.

The main change associated with these new laws is that all functions and powers previously held by INAI have now been transferred to the newly created Ministry of ACGG. It is important to note that all pending matters that were unresolved by INAI will now be handled by the Ministry of ACGG. This will likely result in delays in resolution times and may lead to discrepancies in the criteria applied to resolve cases.

- (2) In October 2024, Senator Juanita Guerra Mena presented to Congress an initiative to enact a Law for Regulating the use of Artificial Intelligence. This initiative seeks to establish a general ethical legal frame for the use of AI systems, ensuring the respect of human rights. This initiative has been neither studied nor approved by the Mexican Congress.
- (3) In April 2024, Senator Ricardo Monreal presented to Congress an initiative for a Federal Law Regulating Artificial Intelligence. This law is aimed at establishing a minimum legal frame for regulating AI systems in Mexico, proposing three levels of risk for classifying AI systems. Authorisation from the competent authority will be required, although the competent authority is not defined. Some sanctions are also included. This initiative has been neither studied nor approved by the Mexican Congress.



Abraham Diaz co-chairs OLIVARES’s Litigation Team, as well as Data Privacy and IT Industry groups, and focuses on trademark law, unfair competition, litigation, trade secrets and plant breeders’ rights, as well as on data privacy matters. His internet experience includes handling domain disputes under the Uniform Domain Name Dispute Resolution Policy (UDRP) and the Local Dispute Resolution Policy (LDRP), as well as providing strategic advice across a range of legal matters.

OLIVARES

Pedro Luis Ogazon 17
San Angel, 01000, Mexico City
Mexico

Tel: +52 55 532 23041
Email: abraham.diaz@olivares.mx
LinkedIn: www.linkedin.com/in/abrahamdiazarceo



Gustavo Alcocer, with more than 35 years of law firm and in-house experience, brings a wealth of knowledge to his domestic and foreign clients at OLIVARES, where he heads the Corporate, Commercial Law Group, and co-chairs the Life Sciences and Data Privacy and IT Industry Groups. His practice focuses on transactional work for companies across IP-intensive industries such as life sciences, information technology, food and beverage, entertainment and sports, transportation and retail.

OLIVARES

Pedro Luis Ogazon 17
San Angel, 01000, Mexico City
Mexico

Tel: +52 55 532 23000
Email: gustavo.alcocer@olivares.mx
LinkedIn: www.linkedin.com/in/gustavo-alcocer-5150b88



Carla Huitron has been a member of the Corporate, Commercial and Privacy Law Group since 2011, providing assistance to national and international clients. Among her work, she supports clients in drafting and reviewing documents such as: service, distribution and merchandise NDAs; franchise and licence agreements; structuring e-commerce, legal frameworks and marketplaces compliance with Data Privacy, company’s by-laws or corporate minutes; and providing legal opinions on civil, commercial and data protection law, among others.

OLIVARES

Pedro Luis Ogazon 17
San Angel, 01000, Mexico City
Mexico

Tel: +52 55 532 23000
Email: carla.huitron@olivares.mx
LinkedIn: www.linkedin.com/in/carla-huitron-piña-076940238

Our mission is to provide innovative solutions and highly specialised legal advice for clients facing the most complicated legal and business challenges in Mexico.

OLIVARES is continuously at the forefront of new practice areas concerning privacy compliance, corporate and commercial law, copyright, litigation, regulatory, anti-counterfeiting, plant varieties, domain names, digital rights and internet-related matters, and the firm has been responsible for precedent-setting decisions in patents, copyrights and trademarks.

Our firm is committed to developing the strongest group of legal professionals to manage the level of complexity and interdisciplinary orientation that clients require. During the first decade of the 21st century, the team successfully led efforts to reshape IP privacy corporate and commercial laws and change regulatory authorisations procedures in Mexico, not only through thought leadership and lobbying efforts, but the firm has also won several landmark and precedent-setting cases at the Mexican Federal and Supreme Courts levels, including in constitutional matters.

Today, the team at OLIVARES includes 11 partners and more than 45 associates working across IP, regulatory, administrative, civil, and

commercial and corporate law and privacy compliance serving many different industries, and is constantly awarded for excellence in legal service.

We aim to utilise every available resource to help clients achieve optimum results, protecting their business interests, IP and other rights at every level and through the applicable administrative or judicial venue, in order to maximise successful outcomes – all while maintaining an overarching goal of contributing to Mexico’s broader stance in the global economy and for the greater good of Mexico’s cultural heritage and its people.

www.olivares.mx



Nigeria

Udo Udoma & Belo-Osagie



Jumoke
Lambo



Chisom
Okolie



Opeyemi
Adeshina



Joel Adeyemi
Adefidipe

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The principal data protection legislation in Nigeria is the Nigeria Data Protection Act 2023 (“NDPA”), which was signed into law by President Bola Ahmed Tinubu on 12 June 2023.

1.2 Is there any other general legislation that impacts data protection?

The following laws and regulations impact data protection in Nigeria:

- The Constitution of the Federal Republic of Nigeria 1999 (as amended) (“Constitution”).
- The NDPA General Application and Implementation Directive (“GAID”), issued by the Nigeria Data Protection Commission (“NDPC”) on 20 March 2025.
- The Nigeria Data Protection Regulation 2019 (“NDPR”).
- The NDPR Implementation Framework 2020 (“NDPR Implementation Framework”), issued by the National Information Technology Development Agency (“NITDA”).
- The Child Rights Act 2003.
- The Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (as amended) (“Cybercrimes Act”).
- The Freedom of Information Act 2011.
- The HIV and AIDS (Anti-Discrimination) Act 2014.
- The NITDA Act 2007.

To address multiple regulatory frameworks on data protection in Nigeria, Article 3 (3) of the GAID provides that, upon the issuance of the GAID, the NDPC shall cease to apply the NDPR 2019 as a legal instrument for regulating data privacy and protection. Further to the highlights of the GAID sent to all Data Protection Compliance Organisations (“DPCO”) by the NDPC, the NDPC stated that the GAID will take effect on 19 September 2025. What this implies is that from 19 September 2025, the NDPR and the NDPR Implementation Framework will cease to be extant laws and will be replaced by the NDPA, which will be read together with the GAID, which will become effective on that date.

1.3 Is there any sector-specific legislation that impacts data protection?

The following sector-specific laws, regulations and guidelines have an impact on data protection in Nigeria:

- The Official Secrets Act 1962.
- The Registration of Telephone Subscribers Regulations 2011, published by the Nigerian Communications Commission (“NCC”).
- The Central Bank of Nigeria (“CBN”) Guidelines on Point-of-Sale Card Acceptance Services 2011.
- The National Health Act 2014.
- The Credit Reporting Act 2017.
- The CBN Regulatory Framework for Bank Verification Number Operations and Watch-List for the Nigerian Banking Industry 2017.
- The Lawful Interception of Communications Regulations 2019, issued by the NCC.
- The Consumer Protection Regulations 2019, issued by the CBN, Nigeria’s apex bank.
- The NITDA Guidelines for Nigerian Content Development in Information and Communication Technology 2019 (as amended).
- The Guidelines for the Management of Personal Data by Public Institutions in Nigeria 2020, issued by the NITDA.
- The Consumer Code of Practice Regulations 2024 published by the NCC.
- Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Banks 2024, issued by the CBN.

1.4 What authority(ies) are responsible for data protection?

The NDPC is the primary data protection authority and is responsible for enforcing the NDPA in Nigeria. The NDPA establishes the NDPC. The NDPC is the agency responsible for enforcing the provisions of the NDPA and the administration of all data protection matters in Nigeria. The NDPA retained and did not repeal the existing NDPR and its Implementation Framework. These documents are to be read in conjunction with the NDPA until the GAID becomes effective. Where there is, however, any conflict in their provisions, the provisions of the NDPA will prevail.

Sector-specific regulatory authorities like the CBN, the NCC, and the Federal Competition and Consumers Protection Commission (“FCCCPC”) may also enforce the various regulations that have an impact on data protection within the sectors that they regulate. The GAID authorises the NDPC to collaborate with other public authorities to ensure compliance with the NDPA.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **“Controller”**
The NDPA defines a “Data Controller” as an individual, private entity, public Commission or agency or any other body who or which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.
- **“Data Breach”**
According to the NDPA, a “Personal Data Breach” means a breach of security of a Data Controller or Data Processor leading to or likely to lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.
- **“Data Controller or Data Processor of Major Importance”**
The NDPA defines a “Data Controller or Data Processor of Major Importance” (“DCPMI”) as a Data Controller or Data Processor that is domiciled, resident in, or operating in Nigeria and processes or intends to process Personal Data of more than such number of Data Subjects who are within Nigeria, as the NDPC may prescribe, or such other class of Data Controller or Data Processor that is processing Personal Data of particular value or significance to the economy, society or security of Nigeria as the NDPC may designate.
- **“Data Subject”**
The NDPA defines a “Data Subject” as an individual to whom Personal Data relates.
- **“Personal Data”**
The NDPA defines “Personal Data” as any information relating to an individual, who can be identified or is identifiable, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, psychological, cultural, social or economic identity of that individual.
- **“Processing”**
The NDPA defines “Processing” as any operation or set of operations which is performed on Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, and does not include the mere transit of data originating outside Nigeria.
- **“Processor”**
According to the NDPA, a “Data Processor” is an individual, private entity, public authority, or any other body, who processes Personal Data on behalf of or at the direction of a Data Controller or another Data Processor.
- **“Sensitive Personal Data”/“Special Categories of Personal Data”**
Under the NDPA, “Sensitive Personal Data” means Personal Data relating to an individual’s:
 - a. genetic and biometric data for the purpose of uniquely identifying a natural person;
 - b. race or ethnic origin;
 - c. religious or similar beliefs, such as those reflecting conscience or philosophy;

- d. health status;
- e. sex life;
- f. political opinions and affiliations;
- g. trade union membership; or
- h. other information prescribed by the NDPC as Sensitive Personal Data.

- **Other key definitions**
The NPDA and the NDPR do not recognise the concepts of “Direct Personal Data” or “Indirect Personal Data”. These concepts are also not recognised under the GAID.
- **“Data Protection Compliance Organisation” (“DPCO”)**
This refers to an entity duly licensed by the NDPC for the purposes of training, auditing, consulting and rendering services and products to ensure compliance with the NDPA or any foreign data protection law that has effect in Nigeria.
- **“Data Portability”**
The NDPR defines data portability as the ability of data to be transferred easily from one IT system or computer to another through a safe and secured means in a standard format.
- **“Data Subject Access Request”**
Under the NDPR, this means the mechanism for an individual to request a copy of their Personal Data under a formal process, which may include the payment of a fee.
- **“Pseudonymisation”**
According to the NDPA, “Pseudonymisation” means the processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person.
- The NDPR also provides for the following key definitions:
 - **“Automated Decision-Making”**
This means a decision based solely on automated processing by automated means, without any human involvement.
 - **“Binding Corporate Rules” (“BCRs”)**
This means Personal Data protection policies and procedures adhered to by the members of a group of firms under common control with respect to the transfer of Personal Data among such members and containing provisions for the protection of such Personal Data.

3 Territorial and Material Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

According to Section 2(2) of the NDPA, the NDPA applies to businesses established in other jurisdictions where they are involved in the processing of the Personal Data of Data Subjects in Nigeria.

3.2 Do the data protection laws in your jurisdiction carve out certain processing activities from their material scope?

Yes. Section 3(1) of the NDPA excludes processing of Personal

Data solely for personal or household purposes from the material scope of the NDPA, provided such processing does not constitute a violation of the fundamental right to privacy of a Data Subject. Nonetheless, in order not to violate the fundamental human right to privacy guaranteed by the Constitution, an individual still has a responsibility to respect the privacy of Data Subjects and can be held accountable if their conduct puts the privacy of a Data Subject at risk.

Furthermore, Section 3 of the NDPA further excludes the following processing activities from the obligations under Part V of the NDPA:

- a. processing activities carried out by a competent authority for the purposes of prevention or investigation, detection, prosecution or adjudication of a criminal offence or the execution of a criminal penalty, in accordance with any applicable law;
- b. carried out by a competent authority for the purpose of the prevention or control of a national public health emergency;
- c. carried out by a competent authority as is necessary for national security;
- d. in respect of publication in the public interest for journalism, educational, artistic and literary purposes to the extent that such obligations and rights are incompatible with such purposes; or
- e. necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.

The exemptions under Section 3 of the NDPA are not absolute. A Data Controller or Data Processor who engages in any one of the exempted data processing activities must still follow the other parts of the NDPA that are not exempted. They are still required to adhere to at least the following sections of the NDPA: the principles of Personal Data processing (Section 24); the lawful basis for Personal Data processing (Section 25); the designation of Data Protection Officers (“DPOs”) (Section 32); Personal Data breaches notification (Section 40); and the entirety of Part VI concerning Data Subjects’ rights. Therefore, while Chapter V of the NDPA is generally exempt (excluding the sections mentioned above), the NDPC will hold a Data Controller or Data Processor responsible for violating any other provision of the NDPA not covered by the exemption. Furthermore, the NDPA also empowers the NDPC to prescribe the types of Personal Data and processing that may be exempted from its application.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

■ Transparency

Section 24(1) of the NDPA provides that Personal Data shall be processed in a fair, lawful and transparent manner. It also provides that Personal Data is to be collected for specified, explicit and legitimate purposes and is not to be further processed in a way incompatible with these purposes. Schedule 1, paragraph 1(ii) of the GAID further clarifies that the principle of transparency entails due disclosure of all material facts that may help a Data Subject and the NDPC to make informed decisions. Data Controllers and Processors may use the Record of Processing Activities in addition to other informational documents, such as the privacy policy required by the NDPA to disclose the material facts.

■ Lawful basis for processing

Section 25 of the NDPA provides six lawful bases for the processing of Personal Data:

- a. where the Data Subject has given and not withdrawn consent for the specific purpose or purposes for which Personal Data is to be processed;
- b. where processing is necessary for the performance of a contract to which the Data Subject is a party or in order to take steps at the request of the Data Subject prior to entering into a contract;
- c. where processing is necessary for compliance with a legal obligation to which the Data Controller or Data Processor is subject;
- d. where processing is necessary in order to protect the vital interests of the Data Subject or of another natural person;
- e. where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official public mandate vested in the Data Controller; or
- f. where processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or Data Processor, or by a third party to whom the data is disclosed.

■ Purpose limitation

The principle of purpose limitation in relation to data protection is set forth in Section 24(1)(b) of the NDPA, which provides that a Data Controller or Data Processor shall ensure that Personal Data is collected for specified, explicit and legitimate purposes, and not further processed in a way that is incompatible with those purposes.

■ Data minimisation

Section 24(1)(c) of the NDPA requires Data Controllers or Data Processors to ensure that Personal Data is adequate, relevant and limited to the minimum necessary for the purposes for which the Personal Data was collected or further processed. Therefore, a Data Controller, when processing Personal Data, must ensure that the Personal Data is adequate and relevant to the purpose(s) for which it is being processed.

■ Proportionality

Please see our answer to the question on data minimisation above.

■ Retention

Section 24(1)(d) of the NDPA provides that a Data Controller or Data Processor shall ensure that Personal Data is retained for not longer than is necessary to achieve the lawful basis for which the Personal Data was collected or further processed. Section 8.2 of the NDPR Implementation Framework specifies the statutory retention periods for storing Personal Data, which will be applicable where no specific duration is agreed between parties or is stated in any applicable law. The retention period stipulated in Section 8.2 of the NDPR Implementation Framework is as follows:

- a. three years after the last active use of a digital platform;
- b. six years after the last transaction in a contractual agreement;
- c. upon the presentation of evidence of death by a deceased’s relative, the Data Controller and/or Processor must immediately delete the Personal Data of the deceased Data Subject unless there is a legal obligation imposed on the Data Controller to continue to store the Personal Data; or

- d. immediately upon a request by the Data Subject or his/her legal guardian, where:
 - i. no statutory provision provides otherwise; and
 - ii. the Data Subject is not the subject of an investigation or suit that may require the Personal Data sought to be deleted.

While the NDPR Implementation Framework further requires that Personal Data, which is no longer in use or which has been retained beyond the requisite statutorily required retention period be destroyed in line with global best practices for such operations, the GAID, on the other hand, stipulates that the storage duration of Personal Data shall lapse not later than six calendar months when the original purpose of the processing has been accomplished, subject to any time-bound obligation of any other law. Based on Article 49(3) of the GAID, whenever it is essential to retain data solely for record purposes, a Data Controller or Data Processor should determine the minimum data that is relevant and necessary for the record purposes. Any residue of data that is not needed should be properly destroyed or irreversibly de-identified. As mentioned above, the GAID is still in its gestation period, which means the provisions of the GAID will become effective from 19 September 2025.

■ **Accuracy**

The NDPA provides that Personal Data must be accurate, complete, not misleading, and, where necessary, kept up to date having regard to the purposes for which the Personal Data is collected or is further processed.

■ **Other key principles**

The NDPA also recognises the following principles:

■ **Data Security**

Section 24(1)(f) of the NDPA provides that a Data Controller or Data Processor shall ensure that Personal Data is processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing, access, loss, destruction, damage, or any form of data breach. Section 39(1) also requires a Data Controller and Data Processor to implement appropriate technical and organisational measures to ensure the security, integrity and confidentiality of Personal Data in its possession.

■ **Accountability**

Section 24(3) provides that a Data Controller or Data Processor owes a duty of care, in respect of data processing, and shall demonstrate accountability, in respect of the principles contained in the NDPA. In addition, the NDPA requires data processing by a third party to be governed by a written contract between the third party and the Data Controller. Accordingly, any person engaging a third party to process the Personal Data obtained from Data Subjects is required to ensure the third party's strict adherence to the terms of such written contracts and the provisions of the NDPA.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

■ **Right of access to (copies of) data/information about processing**

The Data Subject's right to access their Personal Data or copies of such data is guaranteed under Section 34(1)(b)

of the NDPA. Under the NDPA, a Data Subject has the right to obtain from a Data Controller, without constraint or unreasonable delay, a copy of the Data Subject's Personal Data in a commonly used electronic format, except to the extent that providing such data would impose unreasonable costs on the Data Controller, in which case the Data Subject may be required by the Data Controller to bear some or all of such costs. Regulation 3.1 of the NDPR also provides that the Data Controller is required to take appropriate measures to provide any information relating to the data processing to the Data Subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language. This will also apply to information relating to a child. The information is to be provided in writing, or by other means (including electronically or orally, provided that the identity of the Data Subject is proven by some other means, where the information is to be provided orally).

The NDPR also stipulates a maximum period of one month within receipt of the Data Subject's request, to provide the information requested. The Data Controller is to ensure that the information is provided to the Data Subject free of charge. The Data Controller may, however, charge a reasonable fee to cover the administrative costs of providing the information requested by the Data Subject or may refuse to provide the information where the Data Subject's data access request is manifestly unfounded or excessive or is repetitive. The Data Controller may also write a letter to the Data Subject, copying the NDPC, where it refuses to act on the data access request of the Data Subject.

■ **Right to rectification of errors**

Section 34(1)(c) of the NDPA guarantees the right of a Data Subject to request that the Data Controller, correct or if not feasible or suitable, delete the Data Subject's Personal Data that is inaccurate, out of date, incomplete or misleading. According to the GAID, where the error is occasioned by the Data Controller or Processor, the Data Subject is entitled to rectification at no cost.

Under Regulation 3.1(13) of the NDPR, the Data Controller shall also communicate any rectification to each recipient to whom the Personal Data have been disclosed unless this proves impossible or requires a disproportionate effort. The Data Controller is also obligated to inform the Data Subject about those recipients if the Data Subject requests for this disclosure.

■ **Right to deletion/right to be forgotten**

Section 34(1)(d) of the NDPA provides that a Data Subject has the right to request for the erasure of Personal Data concerning the Data Subject, without undue delay. Section 34(2) of the NDPA also provides that the Data Controller shall erase Personal Data without undue delay, where:

- i. the Personal Data are no longer necessary in relation to the purposes for which they were collected or processed; or
- ii. the Data Subject has no other lawful basis to retain the Personal Data.

Regulation 3.1(10) of the NDPR requires the Data Controller who has made the Personal Data public to take all reasonable steps to inform the Data Controllers who are processing the Personal Data of the Data Subject's request to delete the data.

Under Regulation 3.1(13) of the NDPR, the Data Controller is required to also communicate any erasure of Personal

Data to each recipient to whom the Personal Data have been disclosed, unless this proves impossible or involves disproportionate effort. The Data Controller is also obligated to inform the Data Subject about those recipients if the Data Subject requests it.

The GAID provides additional guidance on the right to be forgotten, and provides that a Data Subject has the right to have his Personal Data erased where:

- a. The Personal Data is no longer necessary for the purpose a Data Controller or Data Processor originally collected or processed it.
- b. A Data Controller or Data Processor is relying on an individual's consent as the lawful basis for processing the data and that individual withdraws his or her consent.
- c. A Data Controller or Data Processor is relying on legitimate interest as its justification for processing an individual's data, of which the individual objects to this processing, and there is no overriding legal ground for the organisation to continue with the processing.
- d. A Data Controller or Data Processor is processing Personal Data for direct marketing purposes and the individual objects to this processing.
- e. A Data Controller or Data Processor processed an individual's Personal Data unlawfully.
- f. A Data Controller or Data Processor must erase Personal Data in order to comply with a legal ruling or obligation.

The interests of the Data Controller or Processor may, however, override the rights of a Data Subject under the following circumstances:

- a. The data is used to exercise the right to freedom of expression and information, subject to the limits of derogation permitted under Section 45 of the 1999 Constitution and other safeguards of the NDPA.
- b. The data processing is necessary: (i) to comply with a legal ruling or obligation; (ii) to perform a task carried out in the public interest or when exercising an organisation's official authority; (iii) for public health purposes and to serve the public interest; or (iv) to conduct preventative or occupational medicine (this applies only when the data is processed by a health professional who is subject to a legal obligation of professional secrecy).

■ **Right to object to processing**

Section 36 of the NDPA provides that a Data Subject is entitled to object to the processing of his/her Personal Data. It also provides that the Data Controller shall discontinue the processing of Personal Data, unless the Data Controller demonstrates a public interest or other legitimate grounds, which override the fundamental rights and freedoms, and the interests of the Data Subject. With regard to direct marketing, under the NDPA, once a Data Subject objects, it is absolute, and the Data Controller or Processor is obliged to terminate processing immediately for that purpose.

■ **Right to restrict processing**

Section 34(1)(v) of the NDPA provides that the Data Subject has the right to request for the restriction of processing of its Personal Data or to object to such processing.

Regulation 3.1(11) of the NDPR provides that the Data Subject is entitled to restrict the Data Controller's processing of his/her Personal Data where one of the following applies:

- i. The accuracy of the Personal Data is contested by the Data Subject for a period enabling the Data Controller to verify the accuracy of the Personal Data.
- ii. The processing is unlawful, and the Data Subject opposes the erasure of the Personal Data and requests the restriction of their use instead.
- iii. The Data Controller no longer needs the Personal Data for the purposes of the processing, but they are required by the Data Subject for the establishment, exercise or defence of legal claims.
- iv. The Data Subject has objected to processing, pending the verification whether the legitimate grounds of the Data Controller override those of the Data Subject.

Regulation 3.1(12) also provides that where processing has been restricted, such Personal Data shall, except for the purpose of storage, only be processed with the Data Subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest in Nigeria.

Under Regulation 3.1(13), the Data Controller shall also communicate any restriction on the processing of Personal Data to each recipient to whom the Personal Data has been disclosed, unless this proves impossible or requires a disproportionate effort. The Data Controller is also obligated to inform the Data Subject about the recipients of his/her data where the Data Subject requests for such information.

■ **Right to data portability**

Section 38 of the NDPA gives the Data Subject the right to data portability. It entitles him/her to:

- a. receive Personal Data from a Data Controller in a structured, commonly used and machine-readable format;
- b. transmit Personal Data to another Data Controller without any hindrance; and
- c. have the Personal Data transmitted directly from one Data Controller to another, where technically possible.

The GAID provides that the right to data portability can only be exercised when the legal basis for the processing is consent or contractual necessity. The right is also not applicable against a Data Controller or Data Processor in the performance of its public duties, unless there exists a compelling legitimate interest or right of a Data Subject that may be abridged by reason of denying the Data Subject's right of data portability.

■ **Right to withdraw consent**

Section 35 of the NDPA provides that a Data Subject shall have the right to withdraw, at any time, consent to the processing of his/her Personal Data. The Data Controller is to ensure that it is as easy for the Data Subject to withdraw as to give consent. The withdrawal of consent shall not affect the lawfulness of data processing that occurred before the withdrawal of the consent. Section 26(4) of the NDPA also provides that where the processing of Personal Data is based on the consent of the Data Subject, the Data Subject must be informed of the right to withdraw consent, prior to the granting of consent.

■ **Right to object to marketing**

Section 36(3) of the NDPA provides that where Personal Data is processed for direct marketing purposes, the Data Subject shall have the right to object, at any time, to the processing of the Personal Data concerning the Data

Subject, which includes profiling to the extent that it is related to such direct marketing. Where the Data Subject objects to processing for direct marketing purposes, the Personal Data shall no longer be processed for such purposes.

■ **Right protecting against solely automated decision-making and profiling**

Section 27(g) of the NDPA provides that before a Data Controller collects Personal Data directly from a Data Subject, the Data Controller must inform the Data Subject of the existence of automated decision-making, including profiling, significance, and envisaged consequence of such processing for the Data Subject, and the right to object to and challenge such processing. Section 37 of the NDPA also provides that Data Subjects shall have the right not to be subject to a decision based solely on automated processing of Personal Data, including profiling, which produces legal or similar significant effects concerning the Data Subject.

■ **Right to complain to the relevant data protection authority(ies)**

Data Subjects are entitled under Section 34 of the NDPA to lodge a complaint with the NDPC.

■ **Other key rights**

Under Regulation 3.1(8) of the NDPR, where Personal Data are transferred to a foreign country or to an international organisation, the Data Subject has the right to be informed of the appropriate safeguards for protecting his/her Personal Data in such foreign country.

5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

According to Regulation 4.1(8) of the NDPR, the mass media and civil societies may uphold accountability and foster the objectives of the NDPR. Section 9.1 of the NDPR Implementation Framework provides that, in addition to Data Subjects and government agencies, civil societies or professional organisations may also report a breach of the NDPR to the NDPC.

Under the GAID, a Standard Notice to Address Grievance can be served by:

- a Data Subject directly;
- a person acting under the authority of the Data Subject; or
- a civil society organisation acting in the public interest.

This mechanism explicitly permits not-for-profit organisations to act on behalf of Data Subjects, including seeking remedies or collective redress, particularly when the grievance involves public interest issues.

6 Children’s Personal Data

6.1 What additional obligations apply to the processing of children’s personal data?

Under the NDPA, for the purpose of processing Personal Data, a child is any person below the age of 18. Section 31 of the NDPA requires Data Controllers to apply appropriate mechanisms to verify age and consent, taking into consideration available technology. The presentation of any government-approved identification documents is sufficient for this purpose. Section 31(5) of the NDPA also empowers the NDPC to make regulations relating to the processing of the Personal Data of a child

of 13 years and above in relation to the provision of information and services by electronic means at the specific request of the child.

Where the processing activity of the Data Controller or Processor targets children, the NDPR Implementation Framework imposes an obligation on the Data Controller or Processor to ensure that its privacy policy is made in a child-friendly form with the aim of making the children and their parents/guardians have a clear and easy understanding of the data processing activity before granting their consent to the processing of their child/ward’s Personal Data.

Furthermore, the NDPR prohibits Data Controllers from seeking or accepting consent for processing Personal Data in any circumstance that may violate or endanger a child’s rights.

7 Registration Formalities and Prior Approval

7.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

With respect to registration, the NDPA requires DCPMIs to register with the NDPC within six months after the commencement of the NDPA or on becoming DCPMIs. The NDPC, pursuant to the powers conferred on it under the NDPA, issued a guidance notice which provides further context for determining whether a Data Controller or a Data Processor is a DCPMI (“the Notice”). The Notice was first issued on 14 February 2024 and was updated in the GAID issued on 20 March 2025. DCPMIs are required to register with the NDPC on or before 31 October 2024. Although the registration deadline has passed, registration is still ongoing, subject to the payment of a late registration fee.

The Notice provides that a DCPMI is an entity that keeps or has access to a filing system (whether analogue or digital) for the processing of Personal Data, and:

- a. processes the Personal Data of more than 200 Data Subjects within a six-month period;
- b. provides commercial Information Communication Technology services on any digital device that has storage capacity and belongs to another individual; or
- c. processes Personal Data as an organisation or service provider in the financial, communication, health, hospitality, insurance, e-commerce, public service, education, insurance, export and import, aviation, tourism, oil and gas, or electric power sectors of the economy sectors of the economy.

The Notice creates three classes of DCPMIs based on the levels of Personal Data processed:

- i. Major Data Processing-Ultra High Level (“MDP-UHL”): these are entities that process the Personal Data of over 5,000 Data Subjects in a six-month period. In addition to entities such as commercial banks, telecommunication companies, insurance companies, multinational companies, electricity distribution companies, oil and gas companies, public social media app developers and proprietors, public e-mail app developers and proprietors, communication devices manufacturers, and payment gateway service providers are also deemed to be MDP-UHLs.
- ii. Major Data Processing-Extra High Level (“MDP-EHL”): these are entities that process the Personal Data of over 1,000 Data Subjects within six months. In addition to

entities such as ministries, departments and agencies of government, microfinance banks, higher institutions (Universities, Polytechnics, Colleges of Education etc.), hospitals providing tertiary or secondary medical services, and mortgage banks are also designated as MDP-EHL.

- iii. Major Data Processing-Ordinary High Level ("MDP-OHL"): These are entities that process the Personal Data of over 200 Data Subjects within a six-month period. In addition, entities such as primary and secondary schools, primary health centres, agents, contractors and vendors who engage with Data Subjects on behalf of other organisations/entities (third-party Data Processors) are deemed to be MDP-OHL.

DCPMIs who fail to register with the NDPC before the deadline will be deemed to be in breach of the NDPA and liable to the penalties imposed for non-compliance in the NDPA. Under the NDPA, the penalty imposed on a DCPMI for non-compliance is the payment of a fine of up to 10 million Naira or 2% of the annual gross revenue from the preceding financial year (whichever is the greater of the two sums).

With regard to the notification to the regulator of data processing activities, the NDPR requires a Data Controller or Processor that processes the Personal Data of 2,000 Data Subjects within a 12-month period to file an audit report with the NDPC not later than 15 March every year. The GAID requires every company to conduct periodic compliance audits of their data processing activities to mitigate the risk of data breaches through appropriate technical and organisational measures. Under the GAID, only DCPMIs are required to file a Compliance Audit Return ("CAR") with the NDPC. DCPMIs established before 12 June 2023 are required to file their CAR not later than 31 March each year. Those established after 12 June 2023 are to file CAR not later than 15 months after establishment and shall subsequently file the CAR annually.

The CAR for DCPMIs in the UHL and EHL categories must be filed through a DPCO licensed by the NDPC.

7.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

In order for DCPMI to be registered with the NDPC, they are required to provide the following information:

- a. the name and address of the Data Controller or Data Processor, and the name and address of the DPO of the Data Controller or Data Processor;
- b. the description of Personal Data and the categories and number of Data Subjects to which the Personal Data relate;
- c. the purposes for which Personal Data is processed;
- d. the categories of recipients to whom the Data Controller or Data Processor intends or is likely to disclose Personal Data;
- e. the name and address of any representative of any Data Processor operating directly or indirectly on its behalf;
- f. the country to which the Data Controller or Data Processor intends, directly or indirectly, to transfer the Personal Data;
- g. a general description of the risks, safeguards, security measures and mechanisms to ensure the protection of the Personal Data; and
- h. any other information required by the NDPC.

7.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

Please see our answer to question 7.1 above.

7.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

Both local and foreign legal entities that fall within the scope of the NDPA and the parameters of a DCPMI provided in the Notice are required to register with the NDPC. Nonetheless, as stated in the paragraph 6 of the Notice, the following entities are exempt from the requirement of registration as DCPMI even where they meet the thresholds in the Notice:

- a. Community-Based Associations;
- b. Faith-Based Organisations;
- c. Foreign Embassies and High Commissions;
- d. Judicial establishments or bodies carrying out adjudicatory functions; and
- e. Multigovernmental Organisations. (Although not defined in the GAID, a multigovernmental organisation commonly referred to as an intergovernmental organisation is established by treaty between two or more states to pursue shared objectives. Examples include the United Nations, the African Union, and the World Trade Organization.)

7.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

Please see our answer to question 7.1 above.

7.6 What are the sanctions for failure to register/notify where required?

Please see our response to question 7.1 above.

The NDPA empowers the NDPC to impose fines in respect of a breach of the provisions of the NDPA. The range of fines imposed under the NDPA are as follows:

- a. in the case of a DCPMI, the payment of a fine of 2% of the organisation's annual gross revenue of the preceding year or the payment of the sum of 10 million Naira, whichever is greater; and
- b. in the case of a Data Controller or Data Processor not of Major Importance, the payment of a fine representing 2% of the organisation's annual gross revenue of the preceding year or payment of the sum of 2 million Naira, whichever is greater.

In addition, Section 48 of the NDPA states that the NDPC may also issue enforcement orders including: requiring the Data Controller or Data Processor to remedy the violation; ordering the Data Controller or Data Processor to pay compensation to a Data Subject; ordering the Data Controller or Data Processor to account for the profits realised from the violation, or harm as a result of a violation; or referring the matter to the appropriate regulatory agencies for sanction and to prosecute the organisation.

In determining the applicable sanction(s), the NDPC is required to take into account: (i) the nature, gravity and duration of the infringement; (ii) the purpose of the processing; (iii) number of Data Subjects; (iv) level of damage and any mitigation measures implemented; and (v) intent or negligence; (vi) degree of cooperation with the NDPC; and (vii) types of Personal Data involved.

The NDPC may also institute criminal proceedings where it has determined that an organisation is in breach of the provisions of the NDPA.

7.7 What is the fee per registration/notification (if applicable)?

The registration fees for the three classes of DCPMIs are 10,000 Naira for MDP-OHL, 100,000 Naira for MDP-EHL and 250,000 Naira for MDP-UHL.

In relation to filing the data protection compliance audit, Section 6.3 of the Implementation Framework prescribes the audit filing fees as 10,000 Naira for Data Controllers with less than 2,000 Data Subjects and 20,000 Naira for Data Controllers or Processors with more than 2,000 Data Subjects, respectively.

Under the GAID, the audit returns filing fees have been revised. For UHL DCPMIs, 1 million Naira where the number of Data Subjects whose Personal Data is processed is 50,000 Data Subjects and above, 750,000 Naira for 25,000–49,999 Data Subjects, and 500,000 Naira for below 25,000 Data Subjects. For EHL DCPMIs, 250,000 Naira where the number of Data Subjects whose Personal Data is processed is 10,000 Data Subjects and above, 200,000 Naira for 5,000–2,500 Data Subjects, and 100,000 Naira for below 2,500 Data Subjects. These fees have been announced by the NDPC to take effect from the 2026 audit cycle.

7.8 How frequently must registrations/notifications be renewed (if applicable)?

The Notice states that the registration with the NDPC is to be carried out once. Filing of the CAR is carried out on a yearly basis. Please see our answer to question 7.1 above.

7.9 Is any prior approval required from the data protection regulator?

Prior approval is not required from the NDPC to register as a DCPMI. Approval is also not required from the NDPC to conduct and file a data protection compliance audit.

7.10 Can the registration/notification be completed online?

Yes. The registration of DCPMIs can be done online through the web portal of the NDPC for the registration. Filing of the CAR can also be done online through the web portal of the NDPC.

7.11 Is there a publicly available list of completed registrations/notifications?

The NDPC maintains an online register of organisations that have completed the DCPMI registration on its website. Also, on a yearly basis, the NDPC publishes a list of organisations

that comply with the annual data protection audit and filed their audit report with the NDPC.

7.12 How long does a typical registration/notification process take?

The filing of a data-protection-compliance audit report and the registration as DCPMIs with the NDPC on the online platform can be completed within a day of submitting the online application and the payment of the applicable filing fees.

8 Appointment of a Data Protection Officer

8.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

For DCPMIs, the appointment of a DPO is mandatory. They are obliged under the NDPA to designate a DPO with expert knowledge of data protection law and practices, and the ability to carry out the tasks prescribed under the NDPA and subsidiary legislation made under it. Under the NDPR and the Implementation Framework, every Data Controller is required to designate or appoint a DPO for the purpose of ensuring adherence to the NDPA, relevant data privacy instruments and data protection directives of the Data Controller.

In addition, an organisation that is based in Nigeria would be required to appoint a dedicated DPO who is resident in Nigeria and has full access to the management team in Nigeria, if the organisation falls within the following categories of Data Controllers:

- a. the entity is a government organ, Ministry, Department, institution or Agency;
- b. the core activities of the organisation involve processing Personal Data of over 10,000 Data Subjects per annum;
- c. the organisation processes Sensitive Personal Data in the regular course of its business; or
- d. the organisation possesses critical national information infrastructure (as defined under the Cybercrimes Act or any amendment thereto) consisting of Personal Data.

8.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

The penalties stated in question 7.6 above are applicable.

8.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

The DPO is usually an employee or an external organisation contracted to act in this capacity. As a result, the DPO would be bound by the terms of its employment contract or any contract for service that relates to disciplinary measures or other employment consequences.

8.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

Yes, a business can appoint a single DPO to cover multiple entities, provided this does not impair the DPO's ability to

perform their duties effectively or result in any conflict of interest. The appointment should be made by each of the entities.

Section 3.5 of the Implementation Framework mandates multinational companies with a Nigerian subsidiary to appoint a Nigerian-based DPO, and the DPO of the Nigerian subsidiary may report to a global DPO where such exists. This requirement was not retained under the GAID. While it would appear that the requirement will no longer apply when the GAID comes into effect on 19 September 2025 and the Implementation Framework will cease to be effective, the DCPMI registration rules make it imperative for a person to be appointed as a DPO of a multi-national company to be based in Nigeria. We believe this will continue to be applicable because the requirement for the DPO to provide a Nigerian National Identification Number as part of the DCPMI registration process can only be satisfied by a Nigerian citizen or resident.

8.5 Please describe any specific qualifications for the Data Protection Officer required by law.

Section 32(3) of the NDPA provides that a DPO shall:

- advise the Data Controller or the Data Processor, and their employees, who carry out processing made under the NDPA;
- monitor compliance with the NDPA and related policies of the Data Controller or Data Processor; and
- act as the contact point for the NDPC on issues relating to data processing.

Section 3.7 of the Implementation Framework also provides that a DPO should be chosen with due regard to the nature of the business's processing activities and data protection issues. It further lists the qualities of the DPO to include:

- having professional expertise in Nigerian data protection laws and practices;
- having an in-depth understanding of applicable data protection laws; and
- having the requisite knowledge to do the following:
 - inform and advise the organisation, management, employees and third-party processors of their obligations under the NDPR and the NDPA;
 - monitor compliance with the NDPR, the NDPA and with the organisation's own data protection objectives;
 - assign responsibilities, raise awareness and train members of staff involved in Personal Data processing activities and operations;
 - advise on data protection impact assessments ("DPIA") and monitor its performance; and
 - liaise with the NDPC and/or the DPCO on data protection matters.

Under the GAID, a DPO is required to provide evidence of data protection certification of expertise pursuant to NDPC's annual credential assessment of DPOs. The NDPC's verification of the DPO's certification is the metric for determining if the DPO is fit and proper to carry out the duties contemplated by the NDPA and if the DPO is proficient in safeguarding the rights of Data Subjects at an organisational level.

8.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

Please see our answer to question 8.5 above.

In addition, Article 13(1) of the GAID requires a DPO to prepare semi-annual reports every six months that detail the

data processing activity of the Data Controller or Processor. The report is required to cover all the data processing activities carried out within the six month period.

8.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

Section 44 of the NDPA requires DCPMIs to notify the NDPC of the appointment of the DPO. This information is required at the point of registration, and where there is a change of the DPO, the NDPC must be notified within 60 days of the change.

8.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

The NDPA and the GAID do not expressly require the details of the DPO to be included in the privacy policy. Regulation 3.1(7) of the NDPR lists the identity and contact details of the DPO as part of the information a Data Controller is required to provide to the Data Subject before collecting his/her Personal Data. Therefore, the DPO should be identified in the Data Controller's privacy policy, notice or any equivalent document.

9 Appointment of Processors

9.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes. Section 29(2) of the NDPA requires a Data Controller to enter into a written contract (i.e. a third-party data processing contract) with a third party ("Third-Party Processor") where it engages that third party to process the Personal Data obtained from Data Subjects on its behalf.

9.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

A data processing agreement ("DPA") must be written and signed and must expressly state the roles and obligations of the Data Controller and Third-Party Processor. A DPA must include certain key provisions to ensure adherence to the obligations set out in the NDPA. According to the NDPA, a DPA must clearly indicate that:

- the Data Processor is required to commit to adhering to the data protection principles and obligations applicable to the Data Controller under the NDPA;
- the Processor must assist the controller (or the engaging Processor, if applicable) in fulfilling their obligations to uphold the rights of Data Subjects, including access, correction and deletion requests, among others;
- the Processor must implement adequate security measures to ensure the confidentiality, integrity and overall protection of Personal Data, in line with the provisions of the NDPA;
- the Data Processor undertakes to provide the Data Controller with any information that may reasonably be required to demonstrate compliance with the NDPA; and
- the Data Processor is required to notify the Data Controller if they intend to engage another processor.

The GAID also mandates that DPAs must, at a minimum, contain clauses regarding: (a) the obligations of the Data Controller and Data Processor under the NDPA; (b) the names of the parties; (c) the addresses of the parties; (d) recitals referencing any Principal Agreement or Service Level Agreement; (e) the purpose of data processing; (f) the location of data processing (considering the provisions of the NDPA on cross-border data transfer); (g) the scope of the processing; (h) the lawful bases for data processing; (i) the responsibilities of the parties under the DPA; (j) technical and organisational measures for data protection (if highly technical or scientific, this should be expressly outlined in a schedule to the DPA); (k) the outcome of a DPIA where relevant; (l) potential risks; (m) compliance with the NDPA (evidence of registration with the NDPC should be verified); (n) confidentiality; (o) tenure; (p) specific restrictions; (q) indemnity; (r) insurance; (s) *force majeure*; and (t) dispute resolution. These clauses could be used as guidance in determining the compliance of Data Controller's DPAs.

10 Marketing

10.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

Yes. By virtue of the provision of Section 5.3.1 of the NDPR Implementation Framework, the consent of the Data Subject is required for direct marketing, except where the direct marketing activity is targeted at existing customers of the Data Controllers who have purchased goods or services. Under the GAID, consent is required for direct marketing activities irrespective of whether the Data Subject is an existing customer.

In addition, Section 36(4) of the NDPA provides that where the Data Subject objects to processing for direct marketing purposes, the Personal Data shall no longer be processed for such purposes.

10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

The NDPA does not recognise any B2C or B2B marketing dichotomy with respect to direct marketing. The above restriction will apply to both contexts if they involve the processing of Personal Data of natural persons who are Data Subjects within the provisions of the NDPA. This is because the provisions of the NDPA apply only to the processing activities of the Personal Data of natural persons; that is to say, a Data Subject under the NDPA is a natural person and not a business entity. Any direct marketing activity that is only directed towards artificial persons will not come within the ambit of the NDPA.

10.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

Please see our answer to question 10.1.

10.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Yes, they would apply to direct market activities from other jurisdictions where the Personal Data of Nigerian residents will be processed for such marketing activity. Marketing sent from another jurisdiction implies that the marketers already have the Personal Data of their targets (Data Subjects), which means there had been a prior transfer of the data to that other jurisdiction where the marketer does not directly collect the Personal Data. In such a case, for such a transfer to have been possible, the Data Subject must have consented to the transfer of his/her Personal Data and also to the use or purpose of such transfer.

10.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

Yes. The breach of these marketing restrictions is a breach of the provisions of the NDPA, and the NDPC has the responsibility of enforcing penalties for any breaches of the provisions of the NDPA.

10.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

No, it is not lawful to purchase marketing lists from third parties except where the Data Subject gives his/her consent to the processing of his/her Personal Data for marketing purposes and to the transfer of his/her Personal Data to such third parties. Where a Data Controller intends to transfer the Personal Data of a Data Subject, such Data Controller must ensure that it obtains the consent of the Data Subject according to the provisions of the NDPA.

10.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

The NDPA has a general penalty provision which would also apply where marketing communications are sent in breach of the provisions of the NDPA. Section 49 of the NDPA, in addition to criminal prosecution, prescribes the following penalties for anyone who is found to be in breach of the data privacy rights of any Data Subject:

- a. in the case of a DCPMI, payment of a fine of 2% of its annual gross revenue of the preceding year or payment of the sum of 10 million Naira, whichever is greater; and
- b. in the case of a Data Controller or Data Processor not of Major Importance, payment of the fine of 2% of its annual gross revenue of the preceding year or payment of the sum of 2 million Naira, whichever is greater.

11 Cookies

11.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

According to Section 5.6 of the Implementation Framework, the use of cookies on a website requires consent. A website owner is required to:

- a. make the cookie information clear and easy to understand;
- b. notify users of the presence and purpose of the cookies;
- c. identify the entity responsible for the use of the cookies; and
- d. provide information on how to withdraw consent from the use of the cookies.

The GAID requires that a Data Controller or Processor should display a cookie banner in a manner that is conspicuous and obvious to a user or site visitor.

11.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

While the NDPA and the NDPR are silent on distinguishing different types of cookies, under the GAID, necessary cookies that do not process sensitive data, financial data or any data stored privately by a Data Subject do not need the ticking of a box or similar methods. Necessary cookies are cookies that enable core functionality such as security, network stability management and accessibility. As stated in the GAID, all other forms of cookies require a specific selection of “yes or no” (alternatively: “accept” or “reject”) options presented to the Data Subject.

11.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

We are not aware of any enforcement action that has been taken by the NDPC in relation to cookies.

11.4 What are the maximum penalties for breaches of applicable cookie restrictions?

Please see our answer to question 10.7.

12 Restrictions on International Data Transfers

12.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Personal Data can only be transferred to any other jurisdiction outside Nigeria under any of the mechanisms mentioned in our response to question 12.2.

12.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

In Nigeria, Personal Data can be transferred outside Nigeria in the following circumstances:

- a. the recipient of the Personal Data is subject to a law, BCRs, contractual clauses, code of conduct, or certification mechanism that affords an adequate level of protection with respect to the Personal Data in accordance with the NDPA;
- b. the Data Subject has provided and not withdrawn the consent to such transfer after having been informed of

- the possible risks of such transfers for the Data Subject due to the absence of adequate protection;
- c. the transfer is necessary for the performance of a contract to which a Data Subject is a party or in order to take steps at the request of a Data Subject, prior to entering into a contract;
- d. the transfer is for the sole benefit of a Data Subject; and
 - i. it is not reasonably practical to obtain the consent of the Data Subject to that transfer; and
 - ii. if it were reasonably practicable to obtain such consent, the Data Subject would likely give it;
- e. the transfer is necessary for important reasons of public interest;
- f. the transfer is necessary for the exercise or defence of legal claims; or
- g. the transfer is necessary to protect the vital interests of a Data Subject or of other persons, where a Data Subject is physically or legally incapable of giving consent.

Based on the above, the GAID stipulates that there are three mechanisms of cross-border data transfer:

- a. the adequacy decision by the NDPC;
- b. cross-border data transfer instruments (“CBDTIs”); and
- c. other lawful bases.

Adequacy decision

The NDPC may adjudge a country as affording adequate data protection based on the following conditions stated in Section 42 of the NDPA:

- a. availability of enforceable Data Subject rights, the ability of a Data Subject to enforce such rights through administrative or judicial redress, and the rule of law;
- b. existence of any appropriate instrument between the Commission and a competent authority in the recipient jurisdiction that ensures adequate data protection;
- c. access of a public authority to Personal Data;
- d. existence of an effective data protection law;
- e. existence and functioning of an independent, competent data protection, or similar supervisory authority with adequate enforcement powers; and
- f. international commitments and conventions binding on the relevant country and its membership of any multilateral or regional organisations.

Under the NDPR Implementation Framework, a whitelist of countries deemed to have adequate protection was published. Once the GAID takes effect, that list will no longer be valid.

CBDTIs

These instruments may be referred to as:

- a. codes of conduct;
- b. certifications;
- c. BCRs; or
- d. standard contractual clauses (“SCCs”).

Other lawful bases that could be relied on for cross-border transfer of data are listed in (b)–(g) of the first paragraph of our answer to this question.

12.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

No, registration/notification or prior approval is required to transfer Personal Data to other jurisdictions. Nonetheless, since the NDPC does not have model SCCs and BCRs, if a Data Controller or Processor intends to rely on SCCs and BCRs, it is

advisable that a draft of those documents are shared with the NDPC for review before they are used.

12.4 Do transfers of personal data to other jurisdictions require a transfer impact assessment? If conducting a transfer impact assessment is only mandatory in some circumstances, please identify those circumstances.

No, a Data Controller or Processor is not required to conduct a transfer impact assessment.

12.5 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?

This is not applicable to Nigeria.

12.6 What guidance (if any) has/have the data protection authority(ies) issued in relation to the use of standard contractual/model clauses as a mechanism for international data transfers?

Section 41 of the NDPA and the GAID provide that the Data Controllers and Data Processors can rely on standard contractual/model clauses as a mechanism for international data transfers. No specific guidance has been issued regarding the use of this standard contractual/model clauses, although the NDPC reviews standard contractual/model clauses upon request.

13 Whistle-blower Hotlines

13.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

There are no restrictions on the type of issues that may be reported. Any action amounting to a breach of the NDPA may be reported. According to Section 46 of the NDPA, a Data Subject who is aggrieved by the decision, action or inaction of a Data Controller or Data Processor in violation of the NDPA, or subsidiary legislation made under the NDPA may lodge a complaint with the NDPC.

13.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous reporting is generally permitted.

14 CCTV

14.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

Generally, the use of CCTVs is not treated separately from other forms of Personal Data processing; the NDPA still applies. Where the CCTVs will be deployed in places that may be

accessed by members of the public, a DPIA must be conducted prior to such deployment. If it is found that the deployment of the CCTVs will result in a high risk to the rights and freedoms of Data Subjects, the DPIA must be submitted to the NDPC before their deployment.

In any case, the use of CCTV should ideally be brought to the attention of the Data Subject. The improper use of CCTV can result in a breach of privacy rights. It is recommended that a notice stating that CCTVs are being used should be placed in a conspicuous part of the facility, such as the entrance, so everyone is aware that CCTVs are being used.

14.2 Are there limits on the purposes for which CCTV data may be used?

Yes, the data obtained can only be used for the purpose stated in the CCTV privacy policy. The use of data obtained must abide by the principles of data protection such as fairness, transparency and accountability, among others.

15 Employee Monitoring

15.1 What types of employee monitoring are permitted (if any), and in what circumstances?

There are no specific provisions in the NDPA for employee monitoring. The NDPA, however, applies to any kind of transaction in which the processing of the Personal Data of Nigerian residents is carried out. Any monitoring activity carried out by the employer on the employee should either be pursuant to a provision in their contract of employment, or notice should be given to the employee and their consent obtained before such monitoring is carried out. Such monitoring should not be covert.

15.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Consent is not the only legal basis an employer can rely on to process the Personal Data of employees. The employer could rely on the employment contract where such data processing is permitted in that contract or in the legitimate interest of the business. Where consent is, however, relied on, it must be a freely given, specific, informed and unambiguous indication whether by a written or oral statement or an affirmative action, of the Data Subject's agreement to the processing of Personal Data relating to him/her or to another individual on whose behalf he/she has the permission to provide such consent. Consent is required to be obtained from the Data Subject without fraud, coercion or undue influence, and prior to obtaining such consent, the specific purpose of collection of the Personal Data must be made known to the Data Subject.

Irrespective of the legal bases relied on by the employer for employee monitoring, it must be proportionate, and where possible, the employer should opt for less intrusive monitoring. In addition, the employees must be notified of the monitoring and what data will be collected in the process via a privacy policy.

15.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

The employer has no obligation under the data protection laws to inform the trade union of the steps it takes to monitor its

employees unless it is a provision of a collective bargaining or other agreement with the trade union.

15.4 Are employers entitled to process information on an employee's attendance in office (e.g., to monitor compliance with any internal return-to-office policies)?

Yes, employers are entitled to process information on an employee's attendance in office provided there is compliance with the provisions of the NDPA. We say this because neither the NDPA nor any regulations exclude such processing activities. What is required is for the employer to ensure compliance with the principles of data protection provided in the NDPA.

16 Data Security and Data Breach

16.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Yes, there is. According to Section 39 of the NDPA, a Data Controller and Data Processor shall implement appropriate technical and organisational measures to ensure the security, integrity and confidentiality of Personal Data in its possession or under its control, including protections against accidental or unlawful destruction, loss, misuse, alteration, unauthorised disclosure or access. Hence, both the Data Controller and the Data Processor have the obligation to secure Personal Data. Where data is being transferred to a third party, such transfer will be governed by a contract between both the Data Controller and the third party. The contract will spell out the role of both the Data Controller and the third party in relation to the protection of the data of the Data Subject. It is important to note that under the NDPA, the Data Controller who engages the services of third-party processors remains primarily liable to the Data Subjects for the protection of the Personal Data it collects.

16.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Yes. There is a legal requirement to report a breach to the data protection authority. Section 40 of the NDPA provides that a Data Controller or Processor is expected to report any incident of a breach to the NDPC within 72 hours of becoming aware of the breach. This timeline is required to be documented in the organisation's data protection policy and data privacy policy. The details to be reported include:

- A description of the nature of the Personal Data breach, including the categories and approximate number of Data Subjects and Personal Data records concerned.
- The name and contact details of a point of contact of the Data Controller, where more information can be obtained.
- A description of the likely consequences of the Personal Data breach.
- A description of the measures taken or proposed to be taken to address the Personal Data breach, including,

where appropriate, measures to mitigate its possible adverse effects.

- A description of steps the organisation has taken to reduce the risk of harm to individuals.

In addition to the above, the GAID also provides that the breach notification to the NDPC should also contain the following:

- the date or time period during which the loss or unauthorised access or disclosure occurred;
- an estimate of the number of individuals to whom there is a real risk of significant harm as a result of the loss or unauthorised access or disclosure; and
- a description of any steps the organisation has taken to notify individuals of the loss or unauthorised access or disclosure.

16.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Under Section 40(3) of the NDPA, the Data Controller is required to immediately notify the Data Subject of a Personal Data breach where the breach will likely result in high risks to the freedoms and rights of the Data Subject.

16.4 What are the maximum penalties for personal data security breaches?

The penalties stated in question 7.6 above are applicable.

17 Enforcement and Sanctions

17.1 Describe the enforcement powers of the data protection authority(ies).

- Investigative powers:** Without prejudice to the right of a Data Subject to approach a court of competent jurisdiction for the breach of his/her privacy rights, the NDPC can initiate the investigation of allegations of any breach of the provisions of the NDPA where it appears that the complaint is not frivolous or vexatious. It can invite any party to respond to allegations made against it.
- Corrective powers:** Where the NDPC has ascertained that a Data Controller or Data Processor has violated or is likely to violate any requirement under the NDPA or subsidiary legislation, the NDPC may issue an order for compliance with relevant provisions to curtail further breaches.
- Authorisation and advisory powers:** The NDPC can issue administrative orders to protect the subject matter of an allegation pending the outcome of investigation.
- Imposition of administrative fines for infringements of specified legal provisions:** The NDPC has the power to issue a monetary fine after completing an investigation and being satisfied that a Data Controller or Data Processor has violated any provision of the NDPA or subsidiary legislation. A decision on the money value shall be based on the following considerations:
 - the nature, gravity and severity of the breach;
 - the number of Data Subjects affected;

- iii. the purpose of the processing;
- iv. the level of damage and damage mitigation measures implemented;
- v. the intent or negligence;
- vi. the degree of cooperation with the NDPC; and
- vii. the types of Personal Data involved.

Based on the considerations above, the NDPC can impose fines on any person found to be in breach of the data privacy rights of any Data Subject. Such a person may be liable, in addition to any other criminal liability, to a monetary fine of 2% of the Annual Gross Revenue of the preceding year or payment of the sum of 10 million Naira, whichever is greater, in the case of a DCPMI. For a Data Controller or Data Processor who is not a DCPMI, the penalty is a fine of 2% of the Annual Gross Revenue of the preceding year or the sum of 2 million Naira, whichever is greater.

17.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The NDPC being the data protection authority has the power to make orders for suspension of service by the Data Controller (including processing activities) pending further investigations.

17.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

While specific instances of the NDPC issuing outright bans on data processing activities are not extensively detailed in the available sources, the NDPC’s enforcement actions, including investigations and sanctions, provide context for its approach in terms of general enforcement of the NDPA. Please see our response to question 17.1 for more details on NDPC enforcement actions.

17.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

Yes. The NDPC has investigated and is currently investigating offshore businesses. They are typically served a notice and are required to provide information, as well as attend a Pre-Action Conference, if the investigation progresses to that level.

18 E-discovery/Disclosure to Foreign Law Enforcement Agencies

18.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Businesses respond positively to such a request, subject to the provisions of the NDPA.

18.2 What guidance has/have the data protection authority(ies) issued on disclosure of personal data to foreign law enforcement or governmental bodies?

No guidance has been specifically issued by the NDPC in connection with the disclosure of Personal Data to foreign

enforcement agencies or government bodies; however, Section 25(1)(b)(ii) and (iv) of the NDPA provides that data processing shall be lawful where the processing is necessary for compliance with a legal obligation to which the Data Controller or Data Processor is subject and for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller or Data Processor.

Section 51 of the Cybercrimes Act provides that the Attorney General of the Federation may request or receive assistance from any agency or authority of a foreign State in the investigation or prosecution of offences under the Act and may authorise or participate in any joint investigation or cooperation carried out for the purpose of detecting, preventing, responding and prosecuting any offence under the Act. The Cybercrimes Act further provides that the Attorney General of the Federation may, without prior request, forward to a competent authority of a foreign State information obtained in the course of an investigation, if such information will assist in the investigation of an offence or in the apprehension of an offender under the Act.

Also, Section 5(d) of the Terrorism Act grants powers to law enforcement and security agencies responsible for the gathering of intelligence to establish, maintain and secure communications, both domestic and international, to facilitate the rapid exchange of information concerning acts of terrorism, terrorist financing and proliferation, and proliferation financing.

In addition, Section 90 of the Terrorism Act states that any of the agencies may, on a formal request made by the appropriate authority of a foreign State and with the approval of the Attorney General, disclose to that authority any information in its possession or any other government department, relating to any of the following:

- a. the actions or movements of terrorist entities or persons suspected of involvement in the preparation or the commission of acts of terrorism;
- b. the use of forged or falsified travel papers by persons suspected of involvement in the preparation or the commission of acts of terrorism;
- c. traffic in explosives or other lethal devices or sensitive materials by terrorist entities, groups or persons suspected of involvement in the preparation or the commission of acts of terrorism; and
- d. the use of communication technologies by terrorist entities or persons.

19 Artificial Intelligence

19.1 Are there any limitations on automated decision-making involving the processing of personal data using artificial intelligence?

Yes, there are limitations. Although the NDPA does not specifically provide for the use of artificial intelligence (“AI”), there are rules on automated decision-making. Data Subjects have a right not to be subjected to automated decision-making with legal or similar significant effects concerning the Data Subject. In addition, the Data Subject must be informed in the privacy policy of the existence of automated decision-making and the significance and envisaged consequences of such processing for the Data Subject, as well as the right to object to and challenge such processing.

The GAID provides that the consent of a Data Subject is required before the Data Controller makes a decision based solely on automated processing, which produces legal effects

that concern or significantly affect the Data Subject. This applies where AI is used for automated decision-making.

19.2 What guidance (if any) has/have the data protection authority(ies) issued in relation to the processing of personal data in connection with artificial intelligence?

Under the GAID, AI is categorised under Emerging Technologies (“ETs”), and there are special rules where ETs are used in processing Personal Data. To deploy AI for the processing of Personal Data, a Data Controller or Processor must take the following steps:

- a. Set forth technical and organisational parameters for the processing, taking into account the: (a) right of a Data Subject not to be subject to a decision solely based on automated processes or algorithms; (b) right to be forgotten – and the possibility of using synthetic data or tokenisation of Personal Data which may not be amenable to this right; (c) safeguards for the processing of sensitive Personal Data; (d) safeguards for child rights and other vulnerable groups; (e) regulation of cross-border data flows; and (f) privacy by design and by default.
- b. Document the technical and organisational parameters and include them in the CAR to be filed with the NDPC.
- c. Carry out a DPIA, taking into account assessment of disparate outcomes of data processing, and Data Subjects’ Vulnerability Indexes, as stated in the DPIA. The DPIA must be included in the CAR, which shall be filed with the NDPC.
- d. Determine the suitability of data anonymisation upon collection, either directly from Data Subjects or from any legitimate source, and testing the AI system in low-risk environments where public interest may be served for a reasonable period and where significant outcomes of their use may be observed.
- e. Determine whether there are disparate outcomes and the possibility of effectively addressing the disparate outcomes.
- f. Retool and return (repeatedly as occasions may warrant) to the controlled environment to re-test the AI system until satisfactory outcomes are achieved or a determination may be made to wholly discard the AI system on the ground of unmitigable risk to privacy.
- g. Put in place a mechanism for continuous monitoring and evaluation in all circumstances where AI system may be deployed, if a determination has been made that it is safe for use.

20 Trends and Developments

20.1 In your opinion, what enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.

In 2024, the data protection landscape witnessed an increase in enforcement activities of the NDPC. The NDPC reported¹

that over 1,000 organisations across various sectors were under investigation for the breach of compliance obligations. The NDPC sanctioned four banks and three other institutions for data protection violations, generating over 400 million Naira in fines. The NDPC fined Fidelity Bank PLC 555.8 million Naira for violating the NDPA by processing Personal Data without informed consent and employing non-compliant third-party Data Processors. This decision followed a complaint lodged in April 2023 concerning unlawful data collection for account opening. Despite having opportunities for remediation, the bank failed to present a satisfactory plan, resulting in the fine announced on 21 August 2024.

So far in 2025, the NDPC announced investigations into TikTok and Truecaller for alleged data breaches and violations of the NDPA. According to the NDPC’s National Commissioner and CEO, the NDPC is currently assessing their data handling practices and will take appropriate regulatory action based on its findings.

In addition, the FCCPC issued a fine against WhatsApp LLC and Meta Platforms, Inc. (the “Meta Parties”) in the sum of 220 million US Dollars for, among many other alleged infractions of the law, failing to provide Nigerian users with an option to consent to WhatsApp’s updated privacy policy. Although this enforcement action did not emanate from the NDPC, it was the first time a regulatory authority, which is not the data protection authority, enforced data protection laws. This development reveals that other agencies are capable of enforcing data protection obligations. In April 2025, the Competition and Consumer Protection Tribunal upheld the fine by the FCCPC.

20.2 In your opinion, what “hot topics” are currently a focus for the data protection regulator?

Since the beginning of 2025, the NDPC has clearly evinced the intention to ramp up enforcement. The issuance of the GAID supports this positioning of the regulator, as many data protection obligations were further expounded on to foster compliance. In our opinion, the NDPC is focusing on the registration of DCPMIs. Organisations that fall under this category are encouraged to register with the NDPC as soon as possible and also comply with associated obligations to avoid investigations and penalties from the NDPC.

Endnote

- 1 <https://techpoint.africa/news/ndpc-gets-fines-companies-data-breaches>



Jumoke Lambo is the Managing Partner of Udo Udoma & Belo-Osagie. She also heads the Telecommunications, Media and Technology (“TMT”) team (which includes Data Protection), and she co-heads the firm’s Aviation, Corporate Advisory and Employment (which includes Immigration and Business Establishment) teams. In addition, she oversees Alsec Nominees Limited, the firm’s company secretarial practice. Jumoke was admitted to the Nigerian Bar in 1989 and obtained an LL.B. degree from the University of Bristol in 1988. She joined Udo Udoma & Belo-Osagie as an Associate in 1989, became a Senior Associate in 1998 and was made Partner in 2000. Jumoke is recognised by the Nigerian edition of *Who’s Who Legal* for her M&A practice. Her work has also been noted in the *International Financial Law Review*’s Expert Guides. She was recognised in December 2020 by *BusinessDay* as one of Nigeria’s top 20 female lawyers in business law. In September 2024, *The Guardian* named Jumoke as one of Nigeria’s exceptional and most value-adding female professionals. Jumoke is also a Notary Public.

Udo Udoma & Belo-Osagie
St. Nicholas House (10th, 12th and 13th Floors)
Catholic Mission Street, Lagos Island, Lagos
Nigeria

Tel: +234 1 2774920 / +234 1 2719811 / +234 1 2719812
Email: jumoke.lambo@uubo.org
LinkedIn: www.linkedin.com/in/jumoke-lambo-a55578



Chisom Okolie is a Senior Associate in the firm’s TMT, Banking & Finance and Energy teams. As a professional who understands the law and how it applies to clients’ businesses, she has advised on various areas of the law, including: data protection; debt financing; private equity; corporate re-structuring and M&A; energy; TMT; and entertainment practice. Chisom has co-authored chapters in the *International Comparative Legal Guide* series, Thomson Reuters’ *Practical Law Journal*, and has been recognised for her contributions to the World Bank Group’s *Doing Business Guide* as well as its Women, Business and the Law Report. Due to her continued contributions to the finance and energy sectors, she received a national award as a “Nigerian Rising Star” and one of the “40 leading lawyers under the age of 40” in Nigeria. Chisom has also been acknowledged as a “Rising Star”, “Key Lawyer” and an “Associate to Watch” by international legal ranking institutions, including the *International Financial Law Review*, *The Legal 500* and *Chambers and Partners*.

Udo Udoma & Belo-Osagie
St. Nicholas House (10th, 12th and 13th Floors)
Catholic Mission Street, Lagos Island, Lagos
Nigeria

Tel: +234 1 2774920 / +234 1 2719811 / +234 1 2719812
Email: chisom.okolie@uubo.org
LinkedIn: www.linkedin.com/in/chisom-okolie-a67553b5



Opeyemi Adeshina is an Associate in the firm’s TMT and Energy and Infrastructure teams. He has advised on various areas of the law, including data protection, energy and infrastructure, power, banking and finance, and TMT.

Udo Udoma & Belo-Osagie
St. Nicholas House (10th, 12th and 13th Floors)
Catholic Mission Street, Lagos Island, Lagos
Nigeria

Tel: +234 1 2774920 / +234 1 2719811 / +234 1 2719812
Email: opeyemi.adeshina@uubo.org
LinkedIn: www.linkedin.com/in/opeyemi-alexander-adeshina-447846bb



Joel Adeyemi Adefidipe is an Associate in the firm’s TMT and Capital Market teams. He has advised on various areas of the law, including data protection, TMT, FinTech, banking and finance, and competition. In 2024, Joel was nominated as a Rising Star (Legal) in data protection at PrivCon.

Udo Udoma & Belo-Osagie
St. Nicholas House (10th, 12th and 13th Floors)
Catholic Mission Street, Lagos Island, Lagos
Nigeria

Tel: +234 1 2774920 / +234 1 2719811 / +234 1 2719812
Email: joel.adeyemide@uubo.org
LinkedIn: www.linkedin.com/in/joel-adeyemi-adeyemide-822b05132

Udo Udoma & Belo-Osagie is a full-service law firm that was established over 40 years ago to facilitate corporate and commercial business in Nigeria, across Africa and other jurisdictions in the world across its 21 practice areas. Our firm’s founding and core philosophy is that legal advice should be of the highest possible standard, accessible, commercially-oriented and consistently sound on principle. As a firm, we have developed a reputation for enabling a wide range of transactions, including those that are new to Nigeria, and for generating innovative and practical legal solutions and for facilitating transactions

and resolving disputes, including those that are complex or unusual in our market, within a relatively short space of time.

www.uubo.org



Pakistan

S. U. Khan Associates Corporate & Legal Consultants



Saifullah Khan



Saeed Hasan Khan

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The legislation on data protection is in draft/bill stage and yet to be passed by Parliament. Its title is the Personal Data Protection Bill, 2023 (“the Bill”).

1.2 Is there any other general legislation that impacts data protection?

The Prevention of Electronic Crimes Act, 2016, also contains certain significant provisions about data protection.

1.3 Is there any sector-specific legislation that impacts data protection?

Within the banking sector, the Payment Systems and Electronic Funds Transfers Act, 2007, provides for the secrecy of financial institutions’ customer information; violation is punishable with imprisonment or a financial fine, or both. For the telecoms industry, the Telecom Consumer Protection Regulations, 2009, confer on subscribers of telecoms operators the right to lodge complaints for any illegal practices with the Pakistan Telecommunication Authority (“PTA”), “illegal practices” being a broad term which includes, *inter alia*, illegal use of personal data of subscribers.

1.4 What authority(ies) are responsible for data protection?

Under the Bill, the proposed National Commission for Personal Data Protection of Pakistan would primarily be responsible for data protection.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **“Personal Data”**
“Personal data” means any information that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and

other information in the possession of a data controller, including any sensitive personal data.

Anonymised, encrypted or pseudonymised data which is incapable of identifying an individual is not personal data.

- **“Processing”**
“Processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- **“Controller”**
“Controller” means a natural or legal person or the government, who either alone or jointly has the authority to make a decision on the collection, obtaining, usage or disclosure of personal data.
- **“Processor”**
“Processor” means a natural or legal person or the government who, alone or in conjunction with other(s), processes data on behalf of the data controller.
- **“Data Subject”**
“Data subject” means a natural person who is the subject of the personal data.
- **“Sensitive Personal Data”/“Special Categories of Personal Data”**
“Sensitive personal data” means and includes: financial information, including identification number, credit card data, debit card data, account number or other payment instrument data; health data, including physical, behavioural, psychological and mental health conditions or medical records; computerised national ID card or passport; biometric data; genetic data; religious beliefs; criminal records; political affiliations; caste or tribe; and the individual’s ethnicity.
- **“Data Breach”**
A “Personal Data Breach” is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.
- **Other Key Definitions**
 - “Pseudonymisation” is the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

- “Vital interests” means matters relating to life, fundamental rights, security of a data subject(s), humanitarian emergencies, in particular in situations of natural and man-made disasters, monitoring and management of epidemics.
- “Critical personal data” means such personal data retained by the public service provider – excluding data open to the public. It also includes data identified by sector regulators and classified by the commission as critical and also any data related to international obligations.
- “Significant” means any data controller or processor that is sufficiently great or important to be worthy of attention by its sales revenue, profit, number of employees, market share, capital employed, or any other indicator such as number of users, type of data collected or a combination thereof that may constitute it as significant.

3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The Bill is applicable to data controllers and processors not incorporated in Pakistan (operating digitally or non-digitally in Pakistan) and involved in commercial or non-commercial activity. The Bill is also applicable to data controllers and processors who have no physical appearance in Pakistan but carry out the processing of personal data in a territory where Pakistani law is applicable under public or private international law.

3.2 Do the data protection laws in your jurisdiction carve out certain processing activities from their material scope?

The Bill does not specify any processing activities that are out of the Bill’s material scope; however, it has specified the cases where the processing shall be within the scope of the personal data protection Bill, 2023. The Bill shall be applicable to those data controllers and processors that:

- Are established/registered/present in Pakistan and are processing or authorising the processing of the personal data.
- Have digital presence in Pakistan and are involved in the processing of the personal data concerning any commercial or non-commercial activity but are incorporated outside Pakistan in any other jurisdiction.
- Have no physical presence in Pakistan but are processing personal data of individuals in territories where Pakistani Law is applicable under public and private international law.
- Collect the personal data of data subjects within Pakistan.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
The principle of transparency is not dealt with in the Bill.

- **Lawful basis for processing**
The collection, processing and disclosure of personal data shall only be carried out in compliance with the provisions of the Bill. Personal data shall not be processed unless processed for a lawful purpose directly related to an activity of the data controller (lawful purpose).
- **Purpose limitation**
Personal data shall not be processed unless the processing of the personal data is necessary for, or directly related to, lawful purpose.
- **Data minimisation**
Personal data shall not be processed unless the personal data is adequate; however, the personal data must not be excessive in relation to lawful purpose.
- **Proportionality**
This is not dealt with in the Bill.
- **Retention**
The Bill stipulates that personal data processed for any purpose shall not be kept longer than is necessary for the fulfilment of that purpose. The Bill confers a duty on the data controller to take all reasonable steps to ensure that all personal data are destroyed or permanently deleted if they are no longer required for the purpose for which they were to be processed.
- **Accuracy**
The Bill confers this obligation upon the Data Controller that it must take such adequate steps which must ensure the accuracy of the personal data processed. The Bill makes it obligatory for the Controller to make sure that data processed must be accurate, complete and not misleading and must be kept up to date.
- **Other key principles**
The Bill recognises and provides for consent to be an essential requirement to process personal data of the data subject. The Bill also provides that the data controller may not disclose personal data without the consent of the data subject for any purpose other than the purpose for which the same was to be disclosed at the time of collection or to any third party not earlier notified. The Personal Data Protection Authority protects personal data from any loss or misuse, promote awareness of data protection and deal with complaints. The data controllers/processors who are to be identified as “significant” by the Commission are required to appoint a Data Protection Officer for the sake of the processing of the personal data.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data/information about processing**
The data subject is granted the right of access to personal data, upon payment of a prescribed fee, as to the data subject’s personal data that are being processed by or on behalf of the data controller. The data controller must comply with such data access request within 30 days (extendable to an additional 14 days under certain circumstances). The data subject is entitled to:
 - information as to the data subject’s personal data that are being processed by or on behalf of the data controller; and
 - have communicated to him a copy of the personal data in an intelligible form.

■ **Right to rectification of errors**

In the case that personal data have been supplied to the data subject upon his request and the same are inaccurate, incomplete, misleading or not up to date, or when the data subject knows that his personal data are inaccurate, incomplete, misleading or not up to date, the data subject has the right to get them corrected by making a written request to the data controller.

■ **Right to deletion/right to be forgotten**

The data subject has the right to request that the data controller, without undue delay, erase personal data within 14 days, in the following situations:

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- the data subject withdraws the consent on which the processing is based;
- the data subject objects to the processing;
- the personal data have been unlawfully processed; or
- the personal data must be erased for compliance with a legal obligation.

■ **Right to object to processing**

The data subject has the right to give “data subject notice” in writing to the data controller to:

- i. cease the processing, or processing for a specified purpose or in a specified manner; or
- ii. not begin the processing, or processing for a specified purpose or in a specified manner.

The data subject must state reasons in the “data subject notice” that:

- i. the processing of that personal data or the processing of personal data for that purpose or in that manner is causing, or is likely to cause, substantial damage or distress to him or to another person; and
- ii. the damage or distress is, or would be, unwarranted.

■ **Right to restrict processing**

As explained above.

■ **Right to data portability**

The data subjects have the right to data portability.

■ **Right to withdraw consent**

The data subject has the right to withdraw his consent.

■ **Right protecting against solely automated decision-making and profiling**

The data subject has the right to not be subjected to automated decision-making, including profiling.

■ **Right to complain to the relevant data protection authority(ies)**

The data subject may file a complaint before the proposed National Commission for Personal Data Protection of Pakistan against any violation of personal data protection rights as granted under the Bill, regarding the conduct of any data controller, data processor or their processes which the data subject regards as involving:

- i. a breach of the data subject’s consent to process data;
- ii. a breach of obligations of the data controller or the data processor in the performance of their functions under the Bill;
- iii. the provision of incomplete, misleading or false information while taking consent of the data subject; or
- iv. any other matter relating to protection of personal data.

5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

There is no such right in the Bill.

6 Children’s Personal Data

6.1 What additional obligations apply to the processing of children’s personal data?

The data controller or processor shall process a child’s personal data in such a manner that protects the rights and interests of the child:

- before processing any personal data relating to a child, a data controller or processor must verify the child’s age;
- seek consent of the child’s parent, relevant person or authorised person having parental responsibility over the child to decide on his behalf;
- not process any personal data of a child that is likely to cause the child harm; and
- not subject the child to tracking, behavioural monitoring or targeted advertising.

7 Registration Formalities and Prior Approval

7.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

There is no express requirement in the Bill; however, while discussing the power of the National Commission for Personal Data Protection of Pakistan, the Bill confers upon it the power to devise a registration mechanism for data controllers and data processors. Therefore, the proposed National Commission for Personal Data Protection of Pakistan, when established, will devise the registration requirements. The data controller and data processor, whether digitally or non-digitally operational within the territory of Pakistan, must register with the proposed National Commission for Personal Data Protection of Pakistan in such manner as may be specified by the registration framework to be formulated by the proposed Commission.

Those data controllers and/or data processors who are already registered with any public body shall only be required to intimate the Commission about data processing.

7.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

This aspect will be addressed under the rules to be framed by the proposed National Commission for Personal Data Protection of Pakistan (please see question 7.1 above).

7.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

This aspect will be addressed under the rules to be framed by the proposed National Commission for Personal Data Protection of Pakistan (please see question 7.1 above).

7.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

This aspect will be addressed under the rules to be framed by the proposed National Commission for Personal Data Protection of Pakistan (please see question 7.1 above).

7.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

This aspect will be addressed under the rules to be framed by the proposed National Commission for Personal Data Protection of Pakistan (please see question 7.1 above).

7.6 What are the sanctions for failure to register/notify where required?

This aspect will be addressed under the rules to be framed by the proposed National Commission for Personal Data Protection of Pakistan (please see question 7.1 above).

7.7 What is the fee per registration/notification (if applicable)?

This aspect will be addressed under the rules to be framed by the proposed National Commission for Personal Data Protection of Pakistan (please see question 7.1 above).

7.8 How frequently must registrations/notifications be renewed (if applicable)?

This aspect will be addressed under the rules to be framed by the proposed National Commission for Personal Data Protection of Pakistan (please see question 7.1 above).

7.9 Is any prior approval required from the data protection regulator?

This aspect will be addressed under the rules to be framed by the proposed National Commission for Personal Data Protection of Pakistan (please see question 7.1 above).

7.10 Can the registration/notification be completed online?

This aspect will be addressed under the rules to be framed by the proposed National Commission for Personal Data Protection of Pakistan (please see question 7.1 above).

7.11 Is there a publicly available list of completed registrations/notifications?

This aspect will be addressed under the rules to be framed by the proposed National Commission for Personal Data Protection of Pakistan (please see question 7.1 above).

7.12 How long does a typical registration/notification process take?

This aspect will be addressed under the rules to be framed by the proposed National Commission for Personal Data Protection of Pakistan (please see question 7.1 above).

8 Appointment of a Data Protection Officer

8.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The data controller and/or data processor identified as “significant” by the Commission shall be required to appoint a Data Protection Officer. A Data Protection Officer needs to be well versed in the collection and processing of personal data and the risks associated with the processing.

8.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

There is no specific provision regarding this; however, whosoever shall process any personal data in violation of the provisions of the Bill shall be punished with a fine of up to 125,000 USD or an equivalent amount in Pakistani Rupees.

8.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

The Bill is silent on this aspect. It is expected that further guidelines, in this regard, will be provided under the Rules to be framed by the Commission.

8.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

The Bill is silent on this aspect. It is expected that further guidelines, in this regard, will be provided under the Rules to be framed by the Commission.

8.5 Please describe any specific qualifications for the Data Protection Officer required by law.

No qualifications are prescribed in the Bill. It is expected that further guidelines, in this regard, will be provided under the Rules to be framed by the Commission.

8.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

The Bill is silent on this aspect. It is expected that further guidelines, in this regard, will be provided under the Rules to be framed by the Commission.

8.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

The Bill is silent on this aspect. It is expected that further guidelines, in this regard, will be provided under the Rules to be framed by the Commission.

8.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

The Bill is silent on this aspect. It is expected that further guidelines, in this regard, will be provided under the Rules to be framed by the Commission.

9 Appointment of Processors

9.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

The Bill is silent on this aspect; however, businesses customarily execute an agreement to this effect.

9.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

It is not necessary, under the Bill, to enter into an agreement. However, for the enforcement of an agreement, such formalities must be summarised in writing and registered under the Registration Act, 1908.

10 Marketing

10.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

The Protection from Spam, Unsolicited, Fraudulent and Obnoxious Communication Regulations, 2009, (administered by the PTA) require that all operators (telecom operators licensed by the PTA) establish a standard operating procedure to control spamming. Similarly, all such operators are required to develop a standard operating procedure for controlling unsolicited calls. The operators are also required to establish a consolidated "Do Not Call Register" in connection with controlling unsolicited calls. The operators are further required to ensure registration of telemarketers.

10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

As discussed at question 10.1 above.

10.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

As discussed at question 10.1 above.

10.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?

The restrictions discussed at question 10.1 only apply to operators in Pakistan being licensed by the PTA.

10.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

The PTA is entrusted with monitoring and enforcement as explained at question 10.1 above.

10.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

There is no law regulating this mechanism as such.

10.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Contravention of the Protection from Spam, Unsolicited, Fraudulent and Obnoxious Communication Regulations, 2009, is an offence under the PTA (Re-organization) Act, 1996, punishable with imprisonment which may extend to three years or a fine which may extend to 10 million PKR, or both.

11 Cookies

11.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

The Bill gives the right to data subjects to not be subject to a decision solely based upon automated processing, including profiling.

11.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

The Bill does not distinguish between types of cookies.

11.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

None, in view of there not being any legislation to this effect, and the fact that no data protection authority exists.

11.4 What are the maximum penalties for breaches of applicable cookie restrictions?

None, in view of there not being any legislation to this effect.

12 Restrictions on International Data Transfers

12.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

The Bill provides that if personal data is required to be transferred to any system located beyond the territories of Pakistan or any system that is not under the direct control of the Government of Pakistan, it must be ensured that the country where the data is being transferred offers personal data protection at least equivalent to the protection provided under the Bill. Another basis to transfer data outside is consent of the data subject. Thirdly, personal data may also be transferred outside Pakistan under a framework to be devised by the National Commission for Personal Data Protection of Pakistan. The personal data so transferred shall be processed in accordance with the Bill. Critical personal data shall only be processed in Pakistan.

In the absence of an adequate level of protection, the National Commission for Personal Data Protection of Pakistan may allow the transfer of personal data outside Pakistan as follows:

- Under a binding contract/agreement.
- With the explicit consent of the data subject that has no conflict with the public or national interest of Pakistan.
- International cooperation under any relevant international obligation.
- On conditions to be specified by the National Commission for Personal Data Protection of Pakistan.

12.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

As the law on personal data protection is not yet enforced, businesses typically transfer personal data on the basis of contractual arrangements.

12.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

This is not yet specified in the Bill, although it may be a subject matter of the rules to be framed thereunder.

12.4 Do transfers of personal data to other jurisdictions require a transfer impact assessment? If conducting a transfer impact assessment is only mandatory in some circumstances, please identify those circumstances.

The Bill is silent on transfer impact assessment.

12.5 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?

This is not applicable.

12.6 What guidance (if any) has/have the data protection authority(ies) issued in relation to the use of standard contractual/model clauses as a mechanism for international data transfers?

As the National Commission for Personal Data Protection of Pakistan is not in existence, no such guidance exists.

13 Whistle-blower Hotlines

13.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

The Bill does not have any provision related to “whistle-blowers”. The Public Interest Disclosures Act, 2017, deals with the concept of “whistler-blower”; however, the same primarily deals with and focuses on public sector entities. The said Act has mandated the Government to specify private sector entities (in the official Gazette) to be an “organisation” for the purposes of said Act. Primarily, the Public Interest Disclosures Act, 2017, covers the wilful misuse of power or wilful misuse of discretion by virtue of which substantial loss is caused to the Government or substantial wrongful gain accrues to a public servant or to a third party. As such, the corporate sector is not covered by the Public Interest Disclosures Act, 2017.

13.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

The Bill is silent on this matter; however, anonymous or pseudonymous disclosures are not entertained in terms of Section 3(5) of the Public Interest Disclosures Act, 2017.

14 CCTV

14.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

The Bill does not place or require any registration/notification or prior approval in relation to the use of CCTV.

14.2 Are there limits on the purposes for which CCTV data may be used?

There are no such limits (please see question 14.1 above).

15 Employee Monitoring

15.1 What types of employee monitoring are permitted (if any), and in what circumstances?

The Bill does not have any provision regarding employee monitoring.

15.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

The Bill does not have such requirement. However, consent is generally built-in within the employment contract.

15.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

There is no such requirement.

15.4 Are employers entitled to process information on an employee's attendance in office (e.g., to monitor compliance with any internal return-to-office policies)?

The Bill is silent on this aspect of personal data processing.

16 Data Security and Data Breach

16.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Data controllers, under the Bill, are responsible for taking practical steps to protect personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction.

16.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

The Bill requires the data controller to report a data breach to the National Commission for Personal Data Protection of Pakistan within 72 hours. The exception is where the personal data breach is unlikely to result in a risk to the rights and freedoms of the data subject.

In case the notification is made after 72 hours, the notification must state the reasons for the delay.

The notification must contain the following information:

- Description of the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned.
- Name and contact details of the Data Protection Officer or other contact point where more information can be obtained.

- Likely consequences of the personal data breach.
- Measures adopted or proposed to be adopted by the data controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

16.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

The reporting requirements for the data subjects are the same as explained at question 16.2.

16.4 What are the maximum penalties for personal data security breaches?

Breach	Penalty
A data controller not ceasing the processing of personal data after withdrawal of consent by the data subject.	Fine of 50,000 USD or an equivalent amount in Pakistani Rupees.
Anyone who processes or causes to be processed, disseminates or discloses personal data in violation of this Act.	Fine of up to 125,000 USD or an equivalent amount in Pakistani Rupees, and in case of a subsequent unlawful processing the fine may be raised up to 250,000 USD or an equivalent amount in Pakistani Rupees. In the case of sensitive personal data, the fine is up to 500,000 USD or an equivalent amount in Pakistani Rupees, while, where the offence is related to critical personal data the fine is up to 1 million USD or an equivalent amount in Pakistani Rupees.
Failure to adopt the security measures that are necessary to ensure data security.	Fine of up to 50,000 USD or an equivalent amount in Pakistani Rupees.
Failure to comply with the orders of the National Commission for Personal Data Protection of Pakistan or the court.	Fine of up to 50,000 USD or an equivalent amount in Pakistani Rupees.
Failure to comply with the directions of the National Commission for Personal Data Protection of Pakistan.	Fine of up to 2 million USD or an equivalent amount in Pakistani Rupees. Suspension or termination of the registration and impose additional conditions.
Corporate liability.	Fine of up to 200,000 USD or 1% of annual gross revenue, whichever is higher.

17 Enforcement and Sanctions

17.1 Describe the enforcement powers of the data protection authority(ies).

- (a) **Investigative powers:** The National Commission for Personal Data Protection of Pakistan shall have the powers to decide a complaint, under the Bill, and shall be deemed to be a Civil Court and shall have the same powers as are vested in a Civil Court.
- (b) **Corrective powers:** The National Commission for Personal Data Protection of Pakistan shall have the powers to order a data controller to take such reasonable measures as it may deem necessary to remedy an applicant for any failure to implement the provisions of the Bill. In addition, it shall have the powers to take prompt and appropriate action in response to a data security breach.
- (c) **Authorisation and advisory powers:** Advising the Federal Government and any other statutory authority on measures that must be undertaken to promote protection of personal data and ensuring consistency of application and enforcement of the Bill shall be one of the functions entrusted to the National Commission for Personal Data Protection of Pakistan.
- (d) **Imposition of administrative fines for infringements of specified legal provisions:** As discussed in question 16.4.
- (e) **Non-compliance with a data protection authority:** The National Commission for Personal Data Protection of Pakistan shall have the power to impose a fine of up to 50,000 USD or an equivalent amount in Pakistani Rupees in case anyone fails to comply with its orders. In case of non-compliance with its directions, the fine can be up to 2 million USD or an equivalent amount in Pakistani Rupees.

17.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The Bill is silent on this.

17.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

As the National Commission for Personal Data Protection of Pakistan is not yet in existence, there is nothing to state regarding its approach, nor are there any cases as of yet.

17.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

This is not applicable (please see question 17.3 above).

18 E-discovery/Disclosure to Foreign Law Enforcement Agencies

18.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

The Bill is silent on this aspect; however, generally the foreign law enforcement agencies do not communicate with businesses directly; rather, businesses are contacted via the relevant law enforcement agencies of Pakistan, who coordinate with businesses to respond to foreign law enforcement agencies.

18.2 What guidance has/have the data protection authority(ies) issued on disclosure of personal data to foreign law enforcement or governmental bodies?

As the National Commission for Personal Data Protection of Pakistan is not in existence, no such guidelines exist.

19 Artificial Intelligence

19.1 Are there any limitations on automated decision-making involving the processing of personal data using artificial intelligence?

The Bill rendering a right to data subjects in respect of which the data subject shall have the right to not be subject to a decision solely based on automated processing, which may include artificial intelligence.

19.2 What guidance (if any) has/have the data protection authority(ies) issued in relation to the processing of personal data in connection with artificial intelligence?

As the Bill is yet to be passed by the legislature, no such authority is in existence leading to non-issuance of any guidance.

20 Trends and Developments

20.1 In your opinion, what enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.

There are no enforcement trends that have emerged in Pakistan over the last 12 months.

20.2 In your opinion, what “hot topics” are currently a focus for the data protection regulator?

As the National Commission for Personal Data Protection of Pakistan is not yet in existence, once it comes into force, e-Commerce, banking transactions and telecoms are likely to be the “hot topics” on which the authority is expected to focus.



Saifullah Khan is an international trade, IT and policy lawyer with more than 20 years of diversified and multi-jurisdictional professional experience serving a large client base in the domestic and international markets. His areas of interest include trade remedy laws of the World Trade Organization, customs law, competition law and data privacy. With respect to emerging discipline of data privacy, he advises clients from different jurisdictions on data privacy compliance and cross-border transfer of data. Additionally, he assists clients in the preparation and review of privacy policies and intra-group agreements concerning cross-border transfer of personal data, etc. He is an advocate of the High Court, a member of the Chartered Institute of Arbitrators (UK) and a member of the International Association of Privacy Professionals. He has completed a course at the London School of Economics and Political Science on "Data: Law, Policy and Regulation".

S. U. Khan Associates Corporate & Legal Consultants

First Floor, 92 Razia Sharif Plaza
Fazal-ul-Haq Road, Blue Area
Islamabad, 44000
Pakistan

Tel: +92 51 23447 41/42
Email: saifullah.khan@sukhan.com.pk
LinkedIn: www.linkedin.com/in/saifullahkhan



Saeed Hasan Khan has vast experience advising clients on various issues such as taxation, corporate, regulatory compliance, contractual obligations, etc. and representing them before the authorities. Over the past 20 years, he has practised in direct and indirect taxes, which encompasses all three practice tiers: advisory; execution; and litigation. He advises on cross-border transactions, international tax treaties and matters related to tax due diligence, corporate structures, shareholder agreements and contractual stipulations between the companies. He has developed a keen professional interest in emerging laws about personal data protection and has gained a deep understanding of underlying concepts and principles governing the global data protection laws including the General Data Protection Regulation of the European Union. He carried out a great deal of research on personal data protection laws in various jurisdictions to have a comparison of core legal principles in various jurisdictions. He attended a course at the London School of Economics and Political Science on "Data: Law, Policy and Regulation". He is an Advocate of the High Court, a Member of the Chartered Institute of Arbitrators (UK) and a Member of the International Association of Privacy Professionals.

S. U. Khan Associates Corporate & Legal Consultants

First Floor, 92 Razia Sharif Plaza
Fazal-ul-Haq Road, Blue Area
Islamabad, 44000
Pakistan

Tel: +92 51 23447 41/42
Email: saeed.hasan@sukhan.com.pk
LinkedIn: www.linkedin.com/in/saeed-hasan-khan-1338a63a

S. U. Khan Associates Corporate & Legal Consultants is a pioneering and leading firm practising trade remedy law in Pakistan, with local and international clients. The major service areas include International Trade Law, Data Protection & e-Commerce & IT Law, Competition Law, Foreign Investment Advisory Services, and International Trade Agreements Advisory. The Firm is also a great contributor of professional knowledge to various journals as well as international institutions, such as the United Nations Conference on Trade and Development and the United Nations Commission on International Trade Law (UNCITRAL), etc. The partners have been working closely with the Government in drafting legislations and in policy-making.

www.sukhan.com.pk



Poland

Kieltyka Gładkowski KG Legal



Jakub Gładkowski



Barbara Kieltyka



Malgorzata Kieltyka

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The main sources developing the idea of information protection indicated in Article 51 of the Polish Constitution include Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the General Data Protection Regulation – GDPR) and the Personal Data Protection Act, the aim of which is to supplement and clarify the provisions of the GDPR.

The GDPR and national law apply in parallel – the GDPR regulates the fundamental principles and rights, while the national law specifies exceptions and details in specific sectors.

In addition to the GDPR, Regulation (EU) 2023/2854 of the European Parliament and of the Council on harmonised rules on fair access to data (Data Act) is also key, as it aims to regulate access to **non-personal data**. This act, for example, regulates so-called “connected products”, i.e. smart devices.

1.2 Is there any other general legislation that impacts data protection?

As an extension of the above regulations, the following acts also structurally influence the condition of data circulation:

- a. Polish Act on the Protection of Personal Data Processed in Connection with the Prevention and Combating of Crime.
- b. Polish Electronic Communications Act.
- c. Polish Act on the Protection of Databases.
- d. Polish Act on the exchange of information with law enforcement authorities of EU Member States, third countries, EU agencies and international organisations.
- e. Polish Act on the participation of the Republic of Poland in the Schengen Information System and the Visa Information System.
- f. Polish Act on the Processing of Criminal Information.

1.3 Is there any sector-specific legislation that impacts data protection?

A key example of the dynamic construction of the sectoral structure of regulations is the health service, which includes the Polish Act on Patients’ Rights and the Patient’s Rights Ombudsman, as it defines the rules for processing medical

documentation and protecting sensitive health data, which is currently being covered by the latest data protection umbrella in the comprehensive initiative of Regulation (EU) 2025/327 of the European Parliament and of the Council on the European Health Data Space. The Polish Act on the Health Information System is also important, as it regulates the functioning of IT systems in healthcare, including e-prescriptions, e-referrals, and the Patient’s Internet Account (IKP).

The second striking example of a comprehensive approach to data protection is the banking and finance sector. In this sector, going beyond cybersecurity issues, it is worth mentioning the Polish Banking Law, which concerns the processing of data in connection with the functioning of the banking system, and the Act on Combating Money Laundering and Terrorist Financing (implementing the AML Directive), because it imposes identification obligations and those related to transaction monitoring.

The cross-sectional approach is presented by the Polish employment law system, in which the provisions of the Polish Labor Code, which regulates employee data in the work environment, have a key place. These provisions include sources of whistleblower regulation.

Another obvious example is telecommunications and the Internet, and in this respect, the new Polish Electronic Communications Law, which implements Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) and the Polish Act on the provision of services by electronic means.

The insurance sector also regulates data, including Polish Act on Insurance and Reinsurance Activities, which provides for the rules for processing personal data of insurers’ customers, including health data (e.g. for life insurance policies).

Important legislation from a cross-border perspective in the EU includes the Transport and urban monitoring law, which has important sectoral provisions, including local regulations, and the Act on road transport and public transport, which contains regulations on the processing of passenger data (e.g. in ticket systems) and monitoring in public transport.

1.4 What authority(ies) are responsible for data protection?

In Polish jurisdiction, the President of the Personal Data Protection Office is a state body with the rank of a minister, responsible for supervising the compliance of personal data processing with applicable legal regulations in Poland. His competences include, among others, conducting control proceedings, considering complaints regarding violations of

data protection regulations, as well as issuing administrative decisions in this regard. Decisions may be appealed to an administrative court.

The President manages the work of the Personal Data Protection Office, which has its seat in Warsaw. The legal basis for the establishment of this body is Article 34 of the Personal Data Protection Act.

As for other supervisory authorities (in the EU), the Polish supervisory authority cooperates with the authorities of the 27 EU countries through the European Data Protection Board (EDPB) – the body coordinating the application of the GDPR at the level of the entire Union. The EDPB is an independent body of the EU responsible for the consistent application of the GDPR in all EU Member States since 25 May 2018. It was established under Article 68 of the GDPR and replaced the Article 29 Working Party. For example, the EDPB issues guidelines and recommendations on the application of the GDPR, the most recent of which are Guidelines 02/2025 on processing of personal data through blockchain technologies.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **“Personal Data”**
Personal data is any information relating to an identified or identifiable natural person (data subject); the main definition includes an open catalogue of identifiers. The definition is constantly being improved by the EDPB in the context of the needs of new technologies. The latest guidelines clarify the definition for AI models and include as personal data information that contributes to the identification of a natural person in the context of the operation of technology and software (e.g. consumer profile, risk category, result of a predictive model).
- **“Processing”**
Processing means any operation or set of operations that is performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- **“Controller”**
The controller is generally a natural or legal person, public authority, entity or other entity that, alone or jointly with others, determines the purposes and means of processing personal data.
- **“Processor”**
The processor is a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller.
- **“Data Subject”**
A natural person whose personal data is processed by the controller or processor. This is a differently identified or identifiable natural person based on information as a result of data processing. An example would be a customer, employee, website visitor, prospective customer, patient, student, user, or subscriber.
- **“Sensitive Personal Data”/“Special Categories of Personal Data”**
Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union

membership, as well as genetic data, biometric data used to uniquely identify a natural person, data concerning health, sexuality or sexual orientation of that person.

- **“Data Breach”**
A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
- **Other key definitions**
The above key definitions are created using vague and undefined terms (e.g. “automated”). This causes complications in determining the lawfulness of data processing based on the key definitions. Therefore, there are additional definitions referring to the lawful process of processing or working with data, which define terms such as, for example: “pseudonymization”; “directly or indirectly identifying a person”; “profiling” (the definition emphasises the automation of data processing in order to assess personal factors); or “Automated Decision-Making”. The correction of basic concepts is introduced by periodic interpretative documents of the EDPB. Official documents, such as Guidelines 02/2025 on the processing of personal data through blockchain technologies, make it easier to explain whether, for example, recording data in a blockchain (e.g. signing a contract, placing an order) as a form of recording and sharing data, practically falls within the general definition of data processing under the GDPR (the full text Guidelines can be found at https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-022025-processing-personal-data_en).

3 Territorial and Material Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The main data protection provisions apply when an entity processes personal data and is headquartered in the EU, regardless of where the data is actually processed.

In Poland, personal data protection is regulated mainly by the EU GDPR, as well as the Personal Data Protection Act, and applies to companies outside the EU in the following two cases:

- a. When they offer goods or services to individuals in the EU (even free of charge).
- b. When they monitor the behaviour of individuals within the EU.

The legal basis for this approach is Article 3 of the GDPR.

An obvious practical case is an American company running an online store offering products to customers in Poland.

It should be noted that data protection regulations for both personal and non-personal data can be applied to the common practices of web scraping, i.e. working on data, collecting data using an automatic method, processing data, and parsing data, especially if the entity is headquartered in one country (even outside the EU), the software developers have a base in another country, or the data is collected globally and then sent to a server in yet another jurisdiction.

3.2 Do the data protection laws in your jurisdiction carve out certain processing activities from their material scope?

Yes, the GDPR provides for the exclusion of certain personal data processing activities from its scope. According to Article 2(2) of the GDPR, the provisions of the Regulation do not apply to the processing of personal data in the following situations:

- Processing of data by a natural person as part of activities of a purely personal or household nature (e.g. maintaining a private calendar with contact details).
- Processing of data as part of activities unrelated to EU law (e.g. activities within the framework of national security).
- Processing by EU institutions within the scope of their official functions (regulated in separate legal acts).

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

■ **Transparency**

The principle of transparency is one of the fundamental principles of data processing. It is often referred to in the preamble and articles of the GDPR. The fundamental provision of Article 5(1)(A) of the GDPR focuses on the perspective of transparency **from the point of view** of the data subject (lawfulness, fairness and transparency).

According to the preliminary provisions of this EU regulation, *it should be transparent for individuals that personal data relating to them are being collected, used, accessed or otherwise processed and to what extent such personal data are or will be processed*. Any information related to the processing of such personal data should be easily accessible and understandable and should be presented in clear and plain language.

Furthermore, the principle of transparency requires that any information provided to the public or to data subjects must be concise, easily accessible and understandable, using clear and plain language and, where appropriate, enhanced with visual elements.

In the context of non-personal data, the Data Act also operates on the basis of transparency standards in the relationship between users and entrepreneurs. A key aspect of the transparency principle is the clarity and readability of contracts and trade secrets. The Data Act obliges entrepreneurs to present the conditions for data processing in a way that is understandable and transparent for users. Articles 13 and 14 of the Data Act are important, as well as the implementation of the rights of natural persons (Articles 15–22 and 34 of the Data Act).

Transparency is an important argument in the decisions of supervisory authorities. For example, in case *ZSPR.440.1055.2019* of 5 July 2022, the lack of response from the data controller was considered by the Polish authority to be a violation of the principle of transparency and the information obligation towards the data subject.

■ **Lawful basis for processing**

The legal basis for the processing of personal data is set out in detail in Article 6(1) of the GDPR. Data processing is lawful only if at least one of the following conditions is met:

- consent of the data subject – processing is based on the voluntary, specific, informed and unambiguous consent expressed by the data subject;

- performance of the contract – processing is necessary for the performance of the contract;
- legal obligation incumbent on the administrator (e.g. resulting from tax regulations, labour law);
- protection of the vital interests of a natural person;
- performance of a task carried out in the public interest or in the exercise of public authority; and
- legitimate interest of the administrator or a third party.

■ **Purpose limitation**

It is expressed in Article 5(1)(B) of the GDPR. It states that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is not considered incompatible with the original purposes under Article 89(1).

This principle means, in particular, that the purpose must be specified **before** the processing begins. The controller is not entitled to collect personal data without a clear reason. In addition, the purpose must be clear and lawful – it cannot be hidden, vague or unlawful.

In the Data Act, the purpose limitation principle is implicitly but explicitly expressed, especially in the context of access, sharing and reuse of data. Similar to the GDPR, this principle aims to ensure that data is used only for specific, clearly defined and legitimate purposes that have been made known to the user.

■ **Data minimisation**

The principle of data minimisation is set out in Article 5(1)(C) of the GDPR. It means that personal data must be *adequate, relevant and limited to what is necessary* for the clearly defined purposes for which they are processed. Data controllers should therefore not collect or process more data than is necessary to achieve a specific purpose. The principle of data minimisation for establishing a relationship between the purpose and the scope of data processing means two requirements:

- a. limiting the collection of data to only that which is necessary to achieve the purpose; and
- b. the need to delete data when it becomes unnecessary to achieve the purpose of processing.

The principle of data minimisation is developed in Article 25 of the GDPR, concerning data protection by design and by default. According to this provision, the controller is obliged to implement appropriate technical and organisational measures (e.g. pseudonymisation) at the planning stage of processing, which are intended to effectively implement the principles of data protection, including minimisation.

■ **Proportionality**

In practice, this principle means that the measures taken by the controller must be *appropriate, necessary and not go beyond what is necessary* to achieve the legitimate purpose of processing personal data. Data should not be collected or processed to a greater extent than is necessary to achieve that purpose.

■ **Retention**

The principle of limiting the storage of personal data, expressed in Article 5(1)(E) of the GDPR, imposes on the controller the obligation to store data only for a period no longer than necessary to achieve the purposes for which the data were collected. Personal data should be processed in a form that allows the identification of the

person to whom they relate, only for the time needed to achieve the originally specified purpose, and, after its completion, should be deleted, anonymised or properly archived. An exception to this principle would be situations in which data are stored longer exclusively for archival purposes in the public interest, scientific, historical or statistical research.

Although the Data Act does not contain a direct reference to the principle of limiting data storage, it does establish a number of regulations that, in practice, implement this principle in relation to personal and non-personal data. In particular, the Data Act provides that data may be used and shared only to the extent necessary to achieve specified and agreed purposes. This means that, after these purposes have been achieved, the data should not be further stored or processed, unless there is an express legal or contractual basis for doing so.

Due to the immutable nature of the blockchain, the EDPB in its Guidelines 02/2025 draws attention to the difficulties in implementing the principle of storage limitation, which requires that personal data be stored only for the period necessary to achieve the purposes for which they were collected. The Guidelines suggest that personal data should be stored outside the blockchain (off-chain) or at least in a form that prevents the identification of the data subjects. If it is necessary to store data on the blockchain for its entire existence, the data controller must demonstrate that this is proportionate to the purpose of the processing and document this decision accordingly. In cases where it is technically impossible to delete data from the blockchain, the EDPB recommends using technical measures such as pseudonymisation, encryption or storing data in the form of cryptographic hashes to minimise the risk of violating the rights of data subjects.

■ **Accuracy**

The principle of accuracy is expressly anchored in Article 5(1)(D) of the GDPR. According to its wording, personal data must be accurate and, where necessary, kept up to date, and controllers should take all reasonable steps to ensure that data that are inaccurate, in light of the purposes of their processing, are promptly rectified or erased. It is also important for the controller to take all reasonable steps to erase or rectify data that are inaccurate in light of the purposes of their processing.

Although the Data Act does not directly reference the principle of accuracy within the meaning of the GDPR, it is implied. In particular, this concerns the obligation to ensure the quality, integrity and reliability of data shared within the framework of data sharing between private entities (B2B), public entities (B2G) and users. In this context, data must be accurate because they are the basis for further analyses or decision-making models or used by AI systems.

■ **Other key principles**

The principles of integrity and confidentiality and accountability are key elements of the personal data protection system in the EU.

The principle of **integrity and confidentiality** has been formulated in Article 5(1)(F) of the GDPR, according to which personal data should be processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. This means that the need to ensure the integrity (inviolability) of data and their confidentiality

(protection against access by unauthorised persons). Controllers and processors are obliged to implement data protection measures by design and by default, in accordance with Article 25 of the GDPR.

The principle of **accountability**, regulated in Article 5(2) of the GDPR, means that the controller must not only comply with the principles of personal data protection, but also be able to demonstrate compliance with them. In other words, accountability is the ability of the controller to document and prove that it has implemented appropriate organisational and technical measures to ensure compliance with the provisions of the GDPR.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

■ **Right of access to (copies of) data/information about processing**

The right to access can be divided into the right to obtain information and the right to a copy of data. Based on Article 15 of the GDPR, each data subject may request the data controller to exercise the right to access. This provision entitles the entity to obtain information as to whether their personal data are actually being processed. If the data are being processed, the person requesting information may obtain, among other things, such information as:

1. purposes of processing;
2. the categories of personal data concerned;
3. recipient information;
4. where possible, the planned period for which personal data will be stored;
5. information about the right to request that the controller rectify, delete or limit the processing of data; and
6. information on automated decision-making, including profiling.

■ **Right to rectification of errors**

In the EU Regulation, the right to rectification of data is included in the provision of Article 16, which indicates that the data subject has the right to demand that the controller immediately rectify personal data concerning him or her that are incorrect. Taking into account the purposes of processing, the data subject has the right to demand that incomplete personal data be supplemented, including by submitting an additional declaration. Data rectification may also take place on the basis of proceedings conducted by the President of the Personal Data Protection Office.

■ **Right to deletion/right to be forgotten**

Information on the right to be forgotten appears in the recitals of the GDPR and directly in the provision of the Regulation. In Recital 66 of the GDPR, the emphasis is on strengthening the right to be forgotten on the Internet, and this is to be served by extending the right to erasure by obliging the controller (who has made this personal data public) to inform controllers (who process such personal data) to erase all links to this data, copies of this personal data or replications of it.

Article 17, in turn, indicates that the data subject has the right to demand that the controller delete his or her personal data without delay, and the controller is obliged to delete personal data without undue delay if one of the following circumstances applies:

- 1. personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- 2. the data subject has withdrawn the consent on which the processing is based;
- 3. the data subject files an objection;
- 4. personal data were processed unlawfully; and
- 5. personal data must be erased in order to comply with a legal obligation under Union law or the law of the Member State to which the controller is subject.

■ **Right to object to processing**

According to Article 21 of the GDPR, the data subject is entitled to file an objection. From the moment the objection is filed, the controller is not allowed to process this personal data, except in cases where the controller demonstrates that there are important legitimate grounds for processing, overriding the interests of the rights and freedoms of the data subject or grounds for establishing, pursuing or defending claims. This article also regulates the objection to the use of personal data for direct marketing purposes.

■ **Right to restrict processing**

The right to restrict the processing of personal data is included in Article 18 of the GDPR. According to this provision, the data subject may request the controller to restrict the processing of data in cases such as:

- 1. questioning the accuracy of personal data – for a period enabling the administrator to check the accuracy of such data;
- 2. when the processing is unlawful and the data subject opposes the deletion of personal data and requests the restriction of their use instead; and
- 3. the controller no longer needs the personal data for the purposes of processing, but the data subject requires them for the establishment, exercise or defence of legal claims.

■ **Right to data portability**

The right to data portability is regulated in Article 20 of the GDPR. According to this regulation, the data subject has the right to receive the personal data concerning him or her, which he or she has previously provided to the controller, in a commonly used format. The data subject has the right to transmit this data to another controller if:

- 1. the processing is based on consent or contract; and
- 2. the processing is carried out in an automated manner.

■ **Right to withdraw consent**

The data subject has the right to withdraw previously expressed consent at any time. However, withdrawing consent does not affect the lawfulness of processing that took place before the consent was withdrawn, and the person who consents to the processing of data is informed of this fact before giving consent. The process of withdrawing consent must be as easy as giving it.

■ **Right to object to marketing**

The architecture of the Regulation means that, in the context of the objection principles, marketing should be viewed as a qualified form of general objection to data processing, in this case for marketing purposes. This is confirmed by the position of the President of the Personal Data Protection Office, who issued guidelines that if a person's data are used for marketing purposes, i.e. to present them with an offer of goods or services, they may object to this at any time and if such an objection occurs, their data may no longer be used for such purposes.

■ **Right protecting against solely automated decision-making and profiling**

The process of automated decision-making assumes the exclusion of the human factor, and the processing of personal data is carried out using appropriate technical tools, including AI. This process may, but does not have to, involve profiling.

The data subject (Article 22 of the GDPR) has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning the data subject or significantly affects the data subject in a similar manner. The application of this right does not apply where such processing: is necessary for entering into, or the performance of, a contract between the data subject and the controller; is permitted by Union or Member State law to which the controller is subject and which lays down suitable measures to safeguard the rights, freedoms and legitimate interests of the data subject; or is based on the explicit consent of the data subject.

■ **Right to complain to the relevant data protection authority(ies)**

Legal remedies, liability and sanctions are set out in Chapter VIII of the GDPR, which defines the right to lodge a complaint with a supervisory authority. Every data subject has the right to lodge a complaint with a supervisory authority if they believe that the processing of personal data concerning them infringes the general regulation on personal data. The supervisory authority to which the complaint has been lodged is obliged to inform the complainant about the progress and results of the complaint, including the possibility of seeking a judicial remedy against a legally binding decision of the supervisory authority concerning them.

■ **Right to compensation**

According to Article 82 of the GDPR, any person who has suffered material or non-material damage as a result of a breach of the provisions of the GDPR has the right to obtain compensation for the damage suffered from the controller or processor. It should therefore be noted that in the case of compensation, it may be both material and non-material damage.

5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

Yes. Polish procedural law, such as Article 8 of the Polish Civil Procedure Code or Article 31 of the Polish Code of Administrative Procedure, allows for the possibility of active action to protect the rights of a citizen, including initiating proceedings or admitting to participate in ongoing proceedings. It is important that this is justified by the statutory objectives of such an organisation. In Poland, Non-Governmental Organisations operate mainly in the form of associations and foundations and, in such cases, their objectives (data protection and active participation in individual cases) must be clearly and precisely indicated in their statute registered before the supervisory body.

6 Children's Personal Data

6.1 What additional obligations apply to the processing of children's personal data?

The processing of children's personal data:

- requires special protection (Recital 38 of the GDPR);
- requires all information and communications to be worded in such clear and simple language that a child can easily understand them (Recital 58 of the GDPR);
- requires processing classified as “profiling” to not involve children (Recital 71 of the GDPR); and
- in the case of information society services, the minimum age of consent is 16 years (Article 8 of the GDPR), unless a Member State has set a lower age (at least 13 years).

7 Registration Formalities and Prior Approval

7.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

There is no general obligation to register personal data processing activities with the supervisory authority. Current regulations and procedures are based on the responsibility of data controllers and the principle of so-called “accountability”.

GDPR

The GDPR does not provide for a general obligation to register personal data sets with the supervisory authority.

It introduced the obligation to keep a register of personal data processing activities. This obligation applies to:

- All data controllers and processors employing more than 250 people.
- Smaller entities, if the processing is not occasional, concerns sensitive data or may result in a risk to the rights and freedoms of natural persons (Article 30 of the GDPR).

7.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

Article 30 of the GDPR imposes an obligation to maintain a register of processing activities by data controllers and – to the extent appropriate – also by processors. Although this is not a public register or one requiring notification to the supervisory authority, its scope is clearly defined and is of a detailed nature.

When maintaining such a register, the data controller must include in it, among others:

- The name and surname or name and contact details of the controller and – if any – the joint controllers, the controller’s representative and the Data Protection Officer (DPO).
- Processing purposes and other information.

Similarly, the processor must keep a register that includes the data of the controller, the categories of processing carried out on its behalf, information on international data transfers and the security measures applied.

7.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

Although the register of processing activities is not subject to

notification to the supervisory authority, their internal structure is based on a set of key categories of information. These categories determine how the register is kept and include: legal entity (controller/processor); purpose of processing; category of data; system or database; and data subjects.

Article 30 of the GDPR introduces the obligation to keep a register of processing activities, which is a basic documentation instrument for administrators and processors.

It is crucial that the register is kept in relation to a specific administrator or processor, which means that the organisational criterion is the legal entity that is the party responsible for the processing.

7.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

According to Article 30 of the GDPR, the central category of entities obliged to keep a register of processing activities is the personal data controller. This obligation also applies to the processor, i.e. the one who processes data on behalf of the controller.

In practice, the following entities are obliged to maintain the register:

- Local legal entities established in a given EU Member State.
- Foreign legal entities if they process personal data of persons located in the territory of the EU and offer them goods or services or monitor their behaviour (pursuant to Article 3(2) of the GDPR).
- Representative offices or branches of foreign entities if, as part of their activities, they process data of natural persons from the EU and are subject to the provisions of the GDPR.

The GDPR introduces the so-called “**principle of territorial extension of application**” – controllers and processors outside the EU are covered by the obligations of the GDPR if their activities cover persons located in the Union.

In such cases, in accordance with Article 27 of the GDPR, they are obliged to appoint a representative in the EU who becomes the formal link with the supervisory authority (in Poland, the President of the Personal Data Protection Office).

A representative within the meaning of Article 27 of the GDPR acts on behalf of a controller or processor not established in the EU but whose activities are subject to the GDPR.

7.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

The basic information that must be included in the register is the identification data of the data controller or – in the case of a register kept by a processor – its data and the data of the controller on whose behalf it acts. In particular, these should be:

- Full name of the entity.
- Registered office address.
- Contact details (telephone number, e-mail address, etc.).
- If appointed, contact details of the DPO.
- In the case of controllers or processors outside the EU, details of the representative designated in accordance with Article 27 of the GDPR.

The register must contain a detailed description of the purposes for which personal data are processed. Examples of purposes include: recruitment; HR services; and direct marketing.

The administrator should determine which groups of natural persons are covered by data processing.

The administrator should also specify what type of personal data is being processed. These may include:

- Identification data (name, surname, Personal Identification Number, Tax Number, ID card number).
- Contact details (address, telephone number, e-mail address).
- Location data.
- Health data (special category of data).

Indication of the categories of recipients to whom the data are or may be disclosed is also required.

7.6 What are the sanctions for failure to register/notify where required?

Pursuant to Article 83(4)(A) of the GDPR, infringement of the obligations under Article 30 is subject to administrative fines of up to EUR 10 million or – in the case of an undertaking – up to 2% of the total annual worldwide turnover of the previous financial year, whichever is higher.

Lack of a register can be classified as:

- Infringement of the administrator’s obligations arising from the accountability principle (Article 5(2) of the GDPR).

In one of the decisions of the President of the Personal Data Protection Office (*DKN.5112.14.2022*), a company was fined as much as EUR 132,000 for serious violations of the provisions of the GDPR. The main violation was the failure to include profiling operations in the register of processing activities, which was a violation of Article 30(1) of the GDPR.

7.7 What is the fee per registration/notification (if applicable)?

The GDPR does not provide for a fee for registration or reporting the processing of personal data to the supervisory authority.

Act of 10 May 2018 on the Protection of Personal Data

The Act does not introduce any obligation to register data sets or any fees related thereto.

7.8 How frequently must registrations/notifications be renewed (if applicable)?

The applicable regulations impose on data controllers and processors a continuous obligation to maintain up-to-date documentation regarding data processing, which in practice fulfils the function of accountability and compliance control.

- The document for internal documentation of processing activities is not subject to formal “registration” with the office nor does it require renewal in any time cycles.
- Data administrators are obliged to keep the register up to date.
- The GDPR requires that the register of processing activities be always up to date and available to the supervisory authority (e.g. the President of the Personal Data Protection Office) upon request.

7.9 Is any prior approval required from the data protection regulator?

As a rule, prior approval by the supervisory authority for personal data protection (in Poland, the President of the Personal Data Protection Office) is not required before data processing begins.

However, there are exceptional situations in which prior consultation with the supervisory authority **may be mandatory**. However, these are clearly defined and are of a **supplementary nature**, rather than universal.

The GDPR does not provide for a general obligation to obtain prior approval from a supervisory authority. Instead, the institution of prior consultation with the supervisory authority has been established (Article 36 of the GDPR), which applies only in situations of particular risk to the rights and freedoms of natural persons.

Pursuant to Article 36 of the GDPR, where a data protection impact assessment (DPIA) pursuant to Article 35 of the GDPR indicates a high risk to the rights and freedoms of individuals, and the controller is unable to mitigate the risk by appropriate measures, the controller is required to consult the supervisory authority prior to processing.

Examples of such cases include large-scale monitoring of public spaces (e.g. facial recognition systems), profiling that produces legal effects for individuals, or processing sensitive data (e.g. health, political opinions) in innovative or unusual contexts.

7.10 Can the registration/notification be completed online?

Currently, the personal data controller does not have to “report” anything to the data protection authority before starting to process data, apart from exceptions that concern, among others, high risk and the need for prior consultations (Article 36 of the GDPR). In the supplementary Polish law, electronic channels of contact have been created, including the Electronic Platform of Public Administration Services (EPUAP) – it is possible to submit notifications, inquiries and applications electronically.

7.11 Is there a publicly available list of completed registrations/notifications?

There are legal regulations that provide for the possibility of sharing information on registrations or notifications regarding the processing of personal data, but the availability of this information depends on the legal context and the type of notification.

The GDPR does not provide for a publicly available register that would contain information on all notifications or registrations made by data controllers.

7.12 How long does a typical registration/notification process take?

There is currently no typical formal registration process that ends with confirmation by a supervisory authority.

In some cases, we can speak of reporting activities or formal procedures.

Pursuant to Article 30 of the GDPR, each data controller and, where necessary, the data processor, is obliged to keep a register of data processing activities.

The time required to prepare such a document depends on the complexity of the processing processes in a given organisation, the number of processing operations, the IT systems involved, as well as the experience of the data protection team.

- For a small organisation, preparing a complete register may take several days to several weeks.
- In the case of large companies or public entities, where we are dealing with many departments, processing entities and a variety of data, the process may take several months.

8 Appointment of a Data Protection Officer

8.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

In accordance with Article 37 of the GDPR and Article 9 of the Act of 10 May 2018 on the Protection of Personal Data, the appointment of a DPO is mandatory in three situations:

1. When the processing is carried out by a public authority or a public body (except courts within the scope of their judicial activity).
2. Where the core activity of the controller or processor consists in the **regular and systematic** monitoring of individuals on a large scale.
3. Where the **core** activity consists of **processing special categories of data** (e.g. health data) or criminal conviction data on a large scale.

In other cases, the appointment of a DPO is optional but recommended as good practice.

8.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

Failure to appoint a DPO where this is mandatory constitutes a breach of the GDPR, which may result in the imposition of an administrative fine.

According to Article 83(4)(A) of the GDPR, the fine may amount to up to EUR 10 million or up to 2% of the company's annual worldwide turnover, whichever is higher.

8.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

Yes. Article 38(3) of the GDPR guarantees that the DPO cannot be dismissed or penalised for performing his or her duties.

The DPO must act independently and may not receive instructions on how to perform his or her duties. The employer may not hold him or her liable for any negative consequences for actions taken in accordance with data protection regulations.

8.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

Yes. According to Article 37(2) of the GDPR, one DPO may be appointed for a group of undertakings or several public authorities/entities, provided that he or she is easily accessible

from any place of business. In practice, this means, among other things, the possibility of contact in the local language and accessibility for data subjects.

8.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The GDPR does not specify any specific education or certificates, but Article 37(5) states that the DPO should have appropriate professional knowledge of personal data protection laws and practices and the ability to fulfil the obligations arising from the GDPR.

In practice, experience, knowledge of law and IT systems count, especially in the case of large or complex organisations.

8.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

Article 39 of the GDPR specifies the main tasks of the DPO and the manner of their implementation. The GDPR provides that the DPO is to perform an advisory and supervisory function in the organisation, and its main purpose is to support the data controller and the data processor in ensuring compliance of the processing of personal data with the law.

The basic tasks of the DPO include informing and advising the controller, the processor and the persons who process data, regarding their obligations under the GDPR and other data protection regulations.

Another obligation of the DPO is to support the controller in carrying out DPIA in cases of processing that poses a high risk to the rights and freedoms of natural persons.

8.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

Yes. In accordance with Article 10 of the Personal Data Protection Act, the data controller is obliged to report the DPO's contact details to the President of the Personal Data Protection Office.

The notification is made electronically via a form available on the Personal Data Protection Office website.

8.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

Yes. Articles 13 and 14 of the GDPR require the controller to provide the DPO's contact details in information clauses and documents such as privacy policies.

The purpose of this obligation is to ensure that individuals have easy access to the DPO in the event of questions or requests regarding the processing of personal data.

9 Appointment of Processors

9.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

In accordance with the GDPR, if a company (data controller) entrusts the processing of personal data to an entity processing on its behalf, a personal data processing agreement is mandatory.

9.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

Article 28(3) of the GDPR sets out the essential elements of such an agreement:

- it should be specified in detail for what purpose personal data are processed and to what extent (e.g. customer or employee data);
- the processor may only process data in the manner specified by the data controller in the form of written instructions. The processor may not arbitrarily change the purpose or method of processing; and
- the processor is obliged to implement appropriate technical and organisational measures to ensure the security of the processed data (Article 32 of the GDPR). Data protection measures, such as encryption, pseudonymisation of data, protection against unauthorised access, etc., must be specified.

The agreement should also include, among other things, appropriate technical and organisational measures to protect data against unauthorised access, loss or destruction.

10 Marketing

10.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

The prior consent of the subscriber or end user is, in accordance with the **new** Polish regulation, the basic requirement for the legality of sending commercial information, including direct marketing using automatic calling systems or telecommunications terminal equipment, particularly within the framework of using interpersonal communication services (Article 398 of the Polish Electronic Communications Law).

In the context of the GDPR, electronic marketing as the processing of personal data for marketing purposes (including sending e-mails and text messages) is only legal if the data subject has voluntarily consented to it. This means that the consent to the processing of data for marketing purposes must be given by the data subject (so-called “informed and voluntary consent”).

10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

Yes, the new Polish regulations also apply to B2B marketing, because they refer to the end user without distinction as a private entity or a business entity. The transmission of commercial information, including direct marketing using telecommunications terminal equipment and automated calling systems, is only permissible on the basis of prior consent of the end user or subscriber. This applies to both end users who are natural persons and organisational units.

The prohibition of sending unsolicited commercial and marketing information, mainly by e-mail (spam), but also by telephone and other forms of automated calling systems, applies to messages addressed to a specific recipient: subscriber; or end user.

10.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

Direct marketing is all activities, as well as any related ancillary services, enabling the offering of products or services or the transmission of other information to a group of people – by post, telephone or other direct means – for the purpose of informing them or eliciting a response from the data subject.

The entrepreneur is not allowed to send communications for marketing purposes to the subscriber/consumer without first obtaining consent to such contact.

Automatic calling systems are automated voice communication connections that connect to the end user and transmit a previously prepared recording. Similarly, these may be other messages. Direct marketing and sending unsolicited commercial information may take place in various forms, in particular: e-mail messages; telephone calls to end users; SMS or MMS messages; and any other forms of communication. The **prior consent** of the marketing recipient **is required** for such direct marketing.

10.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Determining whether information is being sent to a subscriber or end user requires analysis of the address information used to send the information. The marketing may use any number or individual electronic address used in electronic communications.

The above restrictions on electronic, telephone and postal marketing therefore also apply to marketing sent from other jurisdictions if the recipient is located in Poland or the EU.

10.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

Yes, the following are appropriate for enforcing violations of marketing restrictions:

1. The President of the Office of Electronic Communications, who conducts proceedings to impose a fine against an entity that uses automatic calling systems or uses telecommunications terminal equipment for the purpose of sending commercial information without prior consent of the subscriber or end user (Article 444, paragraph 1, point 81 of the Polish Electronic Communications Law).
2. The President of the Personal Data Protection Office, who conducts proceedings to impose a fine against an entity that fails to fulfil the obligation to implement technical and organisational protection measures or the information obligation.
3. The President of the Office of Competition and Consumer Protection, because in accordance with the new provision 398, section 4 of the Polish Electronic Communications Law, illegal marketing constitutes an act of unfair competition.

10.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Buying marketing lists from third parties is not strictly prohibited. The requirement for legality is to exercise special caution and comply with the relevant legal regulations.

- a. In the case of purchasing marketing lists, the basic requirement is to ensure that the persons on such a list have consented to the processing of their personal data for marketing purposes (Article 6(1) of the GDPR).
- b. It is important to have an agreement with a third party (processor) that provides such lists.
- c. Before purchasing marketing lists, a risk assessment should be conducted and it should be ensured that opt-out rights are respected.

10.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

As of December 2019, pursuant to Article 445 of the Polish Electronic Communications Law, the President of the Personal Data Protection Office may, by way of a decision, impose a fine of up to 3% of the revenue of the penalised entity achieved in the previous calendar year.

Moreover, illegal use of automatic calling systems or use of telecommunications terminal equipment for the purpose of sending commercial information without prior consent of the subscriber or end user is an act for which a fine calculated on the same basis of 3% is also imposed by the President of the Office of Electronic Communications. It also takes into account the average revenue achieved by a given entity in the three consecutive calendar years preceding the year in which the fine was imposed (Article 446 of the Polish Electronic Communications Law).

Moreover, in the case of spam, the new electronic communications law provides for the possibility of initiating a fine mechanism within the meaning of classic criminal law (Article 448).

The provisions of the GDPR regarding sanctions remain in force, and a separate issue is financial sanctions in the case of proceedings for acts of unfair competition before the Polish Office for Consumer Protection and Competition.

11 Cookies

11.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

In accordance with the new Article 399 of the Polish Electronic Communications Law, the use of cookies and other similar technologies that involve storing information or accessing information already stored in the telecommunications terminal equipment (such as a telephone, computer or tablet) of the subscriber or end user is permitted, provided that:

- a. the subscriber or end user will be informed in advance in a clear, easy and understandable manner about: the purpose of storing and accessing this information; and the possibility of specifying the conditions for storing or accessing this information by means of software settings installed on the telecommunications terminal device used by him, her, or the configuration of the service;
- b. the subscriber or end user, after receiving the said information, consents thereto; and

- c. the stored information or accessing it does not cause any configuration changes in the end user's telecommunications terminal device and the software installed on that device.

In addition, if personal data of users are processed as part of cookies, the GDPR rules on data processing are applicable, including consent, which must be voluntary, specific, conscious and unambiguous, and expressed through active action, e.g. clicking the appropriate acceptance button.

In addition, the EDPB in its Guidelines 05/2020 indicated that the use of so-called "cookie walls" (blocking access to the website without accepting cookies) is inconsistent with the GDPR because it does not provide the user with free choice.

11.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

It is assumed that the new provision mentioned above introducing restrictions on such direct marketing covers all information that is stored in the telecommunications terminal equipment of the subscriber or end user by entities providing telecommunications services or services by electronic means. Therefore, it is indifferent in this respect to distinguish between: essential cookies; functional cookies; analytical (statistical) cookies; and advertising (marketing) cookies.

11.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

Looking at the Polish jurisdiction from the perspective of one of the 27 members of the EU, the greatest potential threat is due to the activity of the most high-profile cases in Europe: *Google LLC* – a fine of EUR 60 million for failing to obtain users' consent to save advertising cookies; and *Microsoft* – a fine of EUR 60 million for failing to collect consent from users from France before placing advertising cookies.

As far as the Polish authority is concerned, one can indicate such actions as warning decisions of the Polish authority for failure to receive the relevant end-user consents (an example of an admonition judicially verified by the Polish Voivodship Administrative Court in Warsaw, reference number: II SA/WA 3993/21).

11.4 What are the maximum penalties for breaches of applicable cookie restrictions?

Under Article 446 of the Polish Electronic Communications Law, the President of the Office of Electronic Communications may, by way of a decision, impose a fine of up to 3% of the revenue of the penalised entity achieved in the previous calendar year.

Moreover, the illegal use of cookies is an act in respect of which the powers of the President of the Polish Office of Electronic Communications also apply to the President of the Office for Personal Data Protection.

The provisions of the GDPR sanctions remain in force, which is a controversial issue in light of the case law of the Polish Administrative Court (perhaps not every cookie file is personal data).

12 Restrictions on International Data Transfers

12.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

According to the GDPR, the transfer of personal data to third countries (outside the European Economic Area – EEA) is only permitted if:

- the European Commission (EC) has issued a decision stating the adequate level of data protection in a given country (so-called “adequacy decision”); or
- other mechanisms provided for in Chapter V of the GDPR have been used (e.g. standard contractual clauses (SCCs), binding corporate rules (BCR)).

If none of these conditions are met, the transfer of data is generally prohibited.

12.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

The most commonly used mechanisms are:

- SCCs approved by the EC.
- The consent of the data subject, given after being informed about the risks.
- Execution of a contract between the controller and the data subject (or taking steps prior to entering into a contract).
- BCR for international capital groups.
- Exceptions provided for in Article 49 of the GDPR, e.g. important reasons of public interest.

12.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

In most cases, prior approval by a supervisory authority is not required if the transfer is based on:

- EC adequacy decision.
- SCCs or BCR (if already approved).

The consent of the supervisory authority may be required if:

- the administrator relies on so-called “*ad hoc* contractual clauses” that have not been approved; or
- wants to rely on so-called “one-off exceptions” (e.g. occasional transfers in the legitimate interest of the controller).

12.4 Do transfers of personal data to other jurisdictions require a transfer impact assessment? If conducting a transfer impact assessment is only mandatory in some circumstances, please identify those circumstances.

Transfer impact assessment (TIA) is mandatory:

- when transferring personal data to a country without an adequacy decision from the EC;

- when using SCCs or other mechanisms; and
- when the recipient country’s laws may undermine GDPR’s protections.

A TIA includes an assessment of whether the law of the recipient country does not effectively limit the enforcement of natural persons’ rights and whether additional protection measures are needed (e.g. encryption, pseudonymisation, end-to-end encryption).

12.5 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?

The Personal Data Protection Office, following the EDPB, indicated:

- controllers must independently assess the level of protection in a third country;
- even when using SCCs, it is necessary to apply additional technical and organisational measures if the recipient’s law does not provide equivalent protection; and
- the need to conduct a TIA and document the risk assessment.

12.6 What guidance (if any) has/have the data protection authority(ies) issued in relation to the use of standard contractual/model clauses as a mechanism for international data transfers?

The Personal Data Protection Office supports the use of new SCCs published by the EC on 4 June 2021.

Recommendations:

- conducting a TIA before implementing SCCs;
- adapting clauses to a specific transfer case (selecting appropriate SCC modules);
- assessment of the adequacy of technical measures (e.g. encryption); and
- maintaining documentation of transfer decisions (accountability principle).

Following the *Schrems II* decision, data protection authorities have published guidelines on the use of SCCs as a data transfer mechanism. The key guidelines are:

- Compliance assessment – companies must conduct a thorough assessment of whether the use of SCCs ensures an adequate level of data protection in the third country.
- Additional protective measures – if standard clauses do not provide sufficient protection, additional protective measures should be taken.
- Documentation and reporting – companies must document their risk assessment and any data protection actions taken.

13 Whistle-blower Hotlines

13.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

In Poland, the new Act of 14 June 2024 on the Protection of Whistleblowers is in force in this respect. The permissible scope of operation of company helplines, also known as ethical

or corporate helplines, includes primarily anonymous, confidential and free receipt of reports from employees.

An oral report made via a recorded telephone line or other recorded voice communication system is documented with the whistleblower's consent in the form of:

1. a recording of the conversation, enabling its retrieval; or
2. a complete and accurate transcript of the conversation prepared by the unit or a designated person.

An oral report made via an unrecorded telephone line or other unrecorded voice communication system is documented in the form of a conversation record.

Reports may be made to various people within the organisation, including superiors, co-workers and other people associated with the company if there is a suspicion of abuse or irregularities.

13.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous reporting of irregularities in companies is generally permitted, but it is not the employer's obligation to accept such reports. The Whistleblower Protection Act does not oblige employers to allow anonymous reports, leaving them free in this matter. However, the employer must clearly state in the procedures whether it accepts anonymous reports and how it will verify them.

Anonymous reports are associated with the risk of abuse, such as false accusations, and difficulties in obtaining additional clarification, which can limit the effectiveness of the investigation. Therefore, companies that decide to accept anonymous reports often implement procedures to minimise these risks, such as an initial assessment of the credibility of the report before a full investigation, and also encourage reporting through open channels that guarantee confidentiality.

14 CCTV

14.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

Currently, in accordance with the GDPR and national regulations (e.g. the Labor Code, Civil Code), the data controller (e.g. a company or a property owner) does not have to register the CCTV system separately with the data protection authority if the monitoring is carried out in accordance with the principles of minimisation and purposefulness of data processing.

The law imposes an obligation to openly inform people staying in the monitored area about the monitoring being conducted. This means that visible signs or information boards about the monitoring must be placed in the place covered by the image recording.

14.2 Are there limits on the purposes for which CCTV data may be used?

The limits are as follows:

- cameras may not record people without their knowledge or consent, especially in private places;

- monitoring should have a legitimate purpose, such as protecting property or ensuring safety, and not be a means of unjustified surveillance;
- in the case of cameras in public places, camera recordings can only be stored for a certain period of time and must be protected from unauthorised access; and
- the people being recorded have the right to access these recordings.

15 Employee Monitoring

15.1 What types of employee monitoring are permitted (if any), and in what circumstances?

In Poland, employee monitoring is permitted, but subject to strict limitations resulting from the Labor Code and personal data protection regulations: the purpose of monitoring must be to ensure safety and work organisation; the monitoring must be proportionate to the purpose it is to achieve; employees must be informed about the scope and purpose of monitoring; and the employer must comply with the principle of data minimisation and have a legal basis for processing personal data.

Permitted types of monitoring and circumstances

- Video monitoring – this can be used to ensure employee safety, property protection, production control and protection of confidential information. Monitoring cannot cover places such as toilets, changing rooms or social rooms. It functions to increase safety, property protection or production control.
- Monitoring activity on a company computer – the employer can monitor the history of Internet browsing, application use, company email, as well as record keyboard and mouse activity or take screenshots. This monitoring applies only to company devices and is intended, among other things, to increase work efficiency.

15.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

The employer does not have to obtain employees' consent to introduce video monitoring in the workplace if the monitoring is used in accordance with Article 222 of the Labor Code, i.e. for purposes such as ensuring employee safety, protecting property, controlling production or protecting confidential information.

However, the employer is obliged to inform employees about the introduction of monitoring at least two weeks before its launch. This notification should include information about:

- the scope of data processing (e.g. which areas are monitored);
- monitoring purposes;
- the method and period of data storage; and
- employee rights related to monitoring.

Typically, notification is provided in written or electronic form (e.g. email, regulations, privacy policy), and may also be announced during a meeting or posted on a notice board.

15.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

The employer is obliged to notify employees about the introduction of monitoring in the manner adopted by a given employer, no later than two weeks before its launch.

In workplaces where employee representatives operate (e.g. works council), the employer should inform them about the planned monitoring and the arrangements for its scope and purpose.

15.4 Are employers entitled to process information on an employee's attendance in office (e.g., to monitor compliance with any internal return-to-office policies)?

Employers have the right to process information regarding an employee's presence in the office, but the scope and method of such monitoring must comply with the provisions of labour law and personal data protection.

Legal bases and limitations

The employer has the right to keep records of the working time and attendance of employees, which is their obligation under the Labor Code. They can do this, for example, through attendance lists, entry registration systems (e.g. access cards) that register the actual time an employee enters and leaves.

16 Data Security and Data Breach

16.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

In the case of personal data, there is a general obligation in Poland and the EU to ensure the security of personal data, which results from the GDPR. It results from Article 5(1)(F) of the GDPR, which states that personal data must be processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organisational measures. Article 32 of the GDPR specifies in detail the obligations in the scope of security of processing, including risk assessment, pseudonymisation, encryption, business continuity, etc. The following are responsible for the security of personal data: the data controller; the entity processing (processor); or the joint controllers.

16.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

There is a legal requirement under Polish and EU law to report personal data breaches to the relevant supervisory authorities.

Article 33 of the GDPR requires the controller to notify the supervisory authority of a personal data breach without undue delay, and no later than 72 hours after the breach has been discovered, unless it is unlikely to result in a risk to the rights and freedoms of natural persons (e.g. if the data has been encrypted and an unauthorised person could not read it). The notification must include at least:

- the nature of the personal data breach (where possible, the categories and approximate number of data subjects and the types and approximate number of data records);
- the name and contact details of the DPO (or other contact person);
- a description of the possible consequences of a violation; and

- a description of the measures taken or proposed by the controller to address the breach, including actions intended to minimise its possible negative effects.

In Poland, personal data breaches may be reported to the President of the Personal Data Protection Office.

In situations where a breach does not meet the criteria for mandatory reporting, but the controller has doubts about the risk assessment, a voluntary report is possible.

16.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Both Polish and EU law require that personal data breaches are reported to data subjects, but only in specific cases. According to Article 34 of the GDPR, the controller is required to notify the data subject immediately of a personal data breach if it is likely to result in a high risk of violating their rights or freedoms. Such a notification must be clear and understandable and should include at least:

- a description of the nature of the breach (e.g. data leakage, loss, access by an unauthorised person);
- the name and contact details of the DPO (if appointed) or other contact point;
- the possible consequences of a breach (e.g. identity theft, financial losses, damage to reputation);
- the measures taken or proposed by the controller to remedy the breach; and
- the recommended actions a person can take to reduce the risk (e.g. changing password, monitoring account activity, contacting their bank, etc.).

The GDPR does not give a specific time period for notifying an individual, but requires this to be done "without undue delay" after the breach has been identified.

Notification to the relevant person is not necessary if the controller has implemented appropriate technical and organisational protection measures that make the data unreadable to unauthorised persons (e.g. encryption).

16.4 What are the maximum penalties for personal data security breaches?

The GDPR provides for two main thresholds for financial penalties:

- up to EUR 10 million or up to 2% of the company's annual worldwide turnover (whichever is higher), for violations such as:
 - failure to keep a record of processing activities;
 - failure to report a data breach to the supervisory authority; and
 - failure to appoint a DPO when required; and
- up to EUR 20 million or up to 4% of the company's annual worldwide turnover – for the most serious infringements, such as:
 - data processing without a legal basis;
 - a lack of consent or its improper obtaining;
 - the violation of the rights of data subjects (e.g. the right to delete data); and
 - the transfer of data to third countries without adequate safeguards.

17 Enforcement and Sanctions

17.1 Describe the enforcement powers of the data protection authority(ies).

(a) Investigative powers

Investigative powers of the enforcement body in Poland include:

- conducting explanatory proceedings (investigations) regarding the application of the GDPR;
- requesting information from the controller or processor and their representatives;
- conducting data protection control, including access to personal data and information necessary to perform tasks;
- obtaining access to premises and technical infrastructure (after appropriate procedures);
- requesting explanations, documents and data related to the processing of personal data; and
- securing evidence, including copies of databases.

(b) Corrective powers

The remedial powers of supervisory authorities are referred to in Article 58(2) of the GDPR and include:

- admonishing the administrator or processor in the event of a breach of the provisions of the GDPR;
- ordering compliance with the data subject's request, e.g. rectification of data, access to data, etc.;
- ordering the adaptation of processing operations to the provisions of the GDPR in a specified manner and within a specified time;
- ordering the controller to notify the data subject of a personal data breach;
- temporarily or definitively restricting processing, including prohibiting it; and
- ordering the rectification or deletion of personal data or restriction of processing (the right to be forgotten).

(c) Authorisation and advisory powers

In the context of EU law, the EDPB and national supervisory authorities have various supervisory authorisations and powers. The most important here are Articles 57 and 58 of the GDPR, which define the tasks and powers of supervisory authorities, as follows:

- advice to controllers and processors (Article 57(1)(C) of the GDPR) – the supervisory authority may advise data controllers and processors, including on DPIAs, and promote good data protection practices; and
- giving opinions on draft legal acts.

The Personal Data Protection Act contains a number of advisory powers of the President of the Personal Data Protection Office, including:

- issuing opinions on draft legal acts – in accordance with Article 60 of the Act, the President of the Personal Data Protection Office may issue opinions on draft normative acts that affect the processing of personal data; and
- supporting public and private entities in the interpretation of regulations – in practice, the President of the Personal Data Protection Office issues guidelines, recommendations, positions and guides regarding the interpretation of GDPR and national regulations.

(d) Imposition of administrative fines for infringements of specified legal provisions

The Personal Data Protection Office imposes fines for violations of GDPR provisions.

(e) Non-compliance with a data protection authority

The Personal Data Protection Office may, for example, use one of the measures provided for in Article 58 of the GDPR (ordering the controller or processor to comply with the GDPR; ordering access to data; issuing a warning or admonition; or ordering compliance with the data subject's requests, etc.). The authority may also impose an administrative fine on a specific entity in the amounts specified in question 16.4. Furthermore, pursuant to Article 82 of the GDPR, the data subject may claim compensation from the controller or processor for damage caused by a breach of the GDPR, including as a result of failure to comply with the authority's instructions.

17.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The Personal Data Protection Office – both under Polish law and EU law – has the right to issue a ban on a specific personal data processing activity. This does not require obtaining a prior court order. Article 58(2)(F) of the GDPR states that the supervisory authority has the right to order the controller or processor to adapt the processing operation to the provisions of the GDPR, order the restriction of the processing of personal data, and order the suspension of the flow of data to a recipient in a third country. These powers are of an administrative nature and may be exercised independently by the supervisory authority. The President of the Personal Data Protection Office may, among other things: prohibit the processing of data; order their deletion; or limit the processing, without the need to obtain a court order. Such decisions may be appealed to an administrative court, but issuing a processing ban does not require prior court consent.

17.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

According to the latest report, the Personal Data Protection Office issued around 2,000 administrative decisions in one year, of which over 90% were cases based on a complaint and not *ex officio*. In half of these cases, it applied remedial measures (Article 58 of the GDPR) and in 300 cases, an injunction. Only 30 cases had penalties.

For 2025, the Personal Data Protection Office has planned sectoral inspections, focusing on areas with a growing risk of personal data breaches and those that are particularly important from a social perspective, i.e. bodies processing personal data in the EU's Large-Scale Systems (including the Schengen Information System and the Visa Information System), as well as entities processing health data.

17.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

Yes, the Personal Data Protection Office exercises its powers towards companies based in other jurisdictions, especially when these companies process the personal data of persons located in the territory of Poland or the EU and are subject to the provisions of the GDPR.

The Personal Data Protection Office cooperates with other data protection authorities in the EU within the so-called "cooperation and coherence mechanism" (one-stop shop),

which allows for the coordination of actions towards entrepreneurs based in other EU Member States. In the case of entrepreneurs from outside the EU, cooperation may take place on the basis of international agreements or other cooperation mechanisms.

18 E-discovery/Disclosure to Foreign Law Enforcement Agencies

18.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Companies check whether the request comes from a legitimate authority and whether it has a legal basis in accordance with local and international data protection and privacy regulations. This often requires analysing whether the request complies with the GDPR or the relevant regulations in the company’s jurisdiction.

Businesses also seek legal advice to assess the scope and validity of the request and to ensure compliance with data protection regulations and to avoid violating the rights of data subjects.

18.2 What guidance has/have the data protection authority(ies) issued on disclosure of personal data to foreign law enforcement or governmental bodies?

Data transfers must be carried out in accordance with national legislation as well as with the provisions of the GDPR (especially Chapter 5), which aims to ensure the continued protection of personal data after their transfer to a third country or an international organisation.

Disclosure of data to law enforcement or government authorities abroad should be based on a legal basis, such as international agreements, mutual understandings or relevant national and EU laws. This must take into account the rulings of the ECJ and the recommendations of supervisory authorities.

19 Artificial Intelligence

19.1 Are there any limitations on automated decision-making involving the processing of personal data using artificial intelligence?

Under Article 21 of the GDPR, the data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or significantly affects him or her in a similar manner.

Examples of restrictions under Regulation (EU) 224/1689 (the AI Act) when using AI systems are:

- the obligation to leave the final decision to the human being (Recital 61);
- the obligation to inform an individual that a high-risk AI system is being used against him or her (Article 26 of the AI Act);
- the obligation to implement monitoring of such decision-making after the introduction of such an AI device to the market; and
- the right of a natural person to be provided with clear and substantive information about the role and the main elements of the decision taken by an entity using an automated decision-making system (Article 86 of the AI Act).

19.2 What guidance (if any) has/have the data protection authority(ies) issued in relation to the processing of personal data in connection with artificial intelligence?

The Personal Data Protection Office follows the guidelines of the EDPB (Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models as of 17 December 2024).

Particularly, regarding anonymisation, the above Opinion states that whether an AI model is anonymous should be assessed on a case-by-case basis by data protection authorities. For a model to be anonymous, it should be very unlikely that (1) the individuals whose data was used to create the model can be directly or indirectly identified, and (2) such personal data can be extracted from the model through queries.

With respect to legitimate interest, the Opinion provides general considerations that data protection authorities should take into account when assessing whether legitimate interest is an appropriate legal basis for the processing of personal data to develop and implement AI models.

If an AI model has been developed on the basis of personal data processed unlawfully, this may affect the lawfulness of its implementation, unless the model has been properly anonymised.

20 Trends and Developments

20.1 In your opinion, what enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.

The following trends can be observed in the enforcement of data protection regulations:

- a significant part of the fines is imposed in connection with the intentional action or omission on the part of the controller, i.e. failure to notify the supervisory authority of a breach of personal data protection or failure to respond to requests from the President of the Personal Data Protection Office;
- the amount of a fine increases with the scale of the incident, i.e. the number of people affected by the violation;
- some of the penalties concern unintentional violations – for example, using IT resources without ongoing support from their manufacturers – resulting from negligence or failure to comply with the obligation to apply appropriate security measures; and
- more severe financial penalties are imposed in cases of data breaches, such as those concerning Personal Identification Numbers or ID cards’ series and numbers.

20.2 In your opinion, what “hot topics” are currently a focus for the data protection regulator?

Poland is working on the final text of the Act on Artificial Intelligence Systems. The main objective of the draft act is to implement the provisions of the AI Act into Polish law. The aim is for supervision of AI systems in Poland to take into account the special position of the supervisory authority for personal data protection, resulting from both the provisions of the AI Act and the GDPR.

The hot topics for the data protection authority are:

- protection of financial data, especially in the shadow banking sector;

- protection of sensitive data, including medical data;
- verification of biased algorithms that form the basis of data processing;
- data protection by design; and
- evaluation of machine data processing in e-commerce.



Jakub Gładkowski is a managing partner and attorney, having qualified in 2013, with full rights of representation before all courts in Poland. He advises clients from a wide variety of sectors, including the: technology; fintech & blockchain; cybersecurity; media & telecommunications; healthcare & life sciences; financial institutions; real estate, construction & infrastructure; transport & logistics; manufacturing; retail & distribution; and energy sectors. He negotiates and drafts contracts in international sales and construction, represents clients in investments processes, M&A, and advises on commodity supply contracts, franchise agreements and joint-venture agreements. He has assisted a number of clients in technology transactions, crowdfunding and virtual currencies. In this respect he has gained experience in a number of legal issues covering compliance, IP and licensing proceedings. He has been involved in robotic process automation contracts and technology licensing structures. He has additional qualifications, including a private detective licence, which facilitates debtors' assets tracing. He has 15 years of experience in commercial and corporate legal matters. He specialises in cross-border transactions and litigation.

Kieltyka Gładkowski KG Legal
Twarda 18, 00-105 Warsaw
Poland

Tel: +48 530 920 011
Email: jg@kg-legal.pl
LinkedIn: www.linkedin.com/in/k-jakub-g%C5%82adkowski-26907277



Barbara Kieltyka was admitted to the Bar in 1982, after entering into the State Commercial Arbitration Register (a central organisational unit of the government from 1949–1989, established to resolve disputes over property rights, establish legal relations, ensure discipline in the implementation of national economic plans and ensure the implementation of contracts concluded between economic entities). She is a licensed receiver and a veteran of corporate, banking and energy law, with 45 years of legal experience. She has more than 20 years' experience in-house at the Thermal Power and Energy Enterprise, where she litigated numerous court cases – civil, criminal, administrative and employment – in all instances, including at the Supreme Court and the Supreme Administrative Court. She acted as an in-house lawyer for the biggest Polish bank for almost 20 years, where she worked with international clients, assisted in difficult negotiations, litigated cases and assisted in restructuring and debt collection of difficult loans. She rendered assistance to the State Archives, dealing with complex documents and public procurement cases.

Kieltyka Gładkowski KG Legal
Sw. Anny 9, 31-008, Krakow
Poland

Tel: +48 122 634 674
Email: bk@kg-legal.pl
URL: www.kg-legal.eu



Malgorzata Kieltyka is a partner and attorney, with full rights of audience in all courts in Poland. She has been a practising lawyer since 2008 and is ranked among the leading individuals in healthcare & life sciences sector by *The Legal 500 EMEA 2020* (<https://www.legal500.com/firms/232083-kieltyka-glادkowski-kg-legal/c-poland/lawyers/4391814-magorzata-kieltyka>). She represents mostly international clients operating in various sectors, such as pharmaceuticals, new technologies, IT, media, healthcare & life sciences, transport & logistics, telecommunications, and financial institutions, including fintech and start-ups. She deals with commercial law, formation of companies, handles M&A transactions, corporate restructuring, corporate governance and provides ongoing advice to corporate clients. She extensively advises on life science and technology transactions and litigation. In that respect, she has extensive experience in regulatory and commercial issues involving pharmaceuticals, medical devices, cosmetics, foods, including novel foods and borderline products. She handles entry procedures, labelling, advertising matters (including competition aspects) and advises on sales models.

Kieltyka Gładkowski KG Legal
Sw. Anny 9, 31-008, Krakow
Poland

Tel: +48 501 648 500
Email: mk@kg-legal.pl
LinkedIn: www.linkedin.com/in/malgorzata-kieltyka-021425156

Kieltyka Gładkowski KG Legal is a full-service Polish law firm, with offices in Warsaw, Krakow and with an address office in New York in the One World Trade Center (<https://www.istart1.com>). We also have a unit branch in the city near the border with Ukraine. The team comprises more than 30 lawyers. Our law firm is made up of Polish lawyers with an international background, including still active veteran banking and energy attorneys, practising law since 1982.

Kieltyka Gładkowski KG Legal handles mainly cross-border cases. It has a dedicated corporate and private client desk. We advise international and domestic clients on the basis of Polish law, in litigation and in non-contentious matters.

Our particular focus is on cross-border and multi-jurisdictional matters, primarily within the international trade; technology; technology transfers, IP/IT, TMT, fintech & blockchain; cybersecurity; AI data centres, media & telecom; healthcare & life sciences; digital health; financial

institutions; DeFi; defence; real estate, construction & infrastructure; transport & logistics; e-commerce; manufacturing; and retail & distribution sectors, apart from standard areas of expertise like corporate, commercial, antitrust & competition, bankruptcy, commercial litigation, energy and employment.

We offer services within enforcement of judgments, bankruptcy and asset tracing, including services in crypto asset tracing.

www.kg-legal.eu



Saudi Arabia



Saifullah Khan



Saeed Hasan Khan

Droua Al-Amal Consultants

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The principal data protection law in the Kingdom of Saudi Arabia (the Kingdom) is the Personal Data Protection Law (PDPL), issued pursuant to Royal Decree No. M/19 dated 09/02/1443 AH, corresponding to 16 September 2021. The law was enforced on 14 September 2023; however, a grace period of one year, i.e. until 14 September 2024, has been granted to entities, to comply with the data privacy law.

The implementing regulations of the PDPL have also been issued, which have elaborated the principles of the PDPL. In addition, the Regulation on Personal Data Transfer outside the Kingdom has also been issued, which allows the transfer of personal data outside the Kingdom, subject to certain requirements.

1.2 Is there any other general legislation that impacts data protection?

The Basic Law of Governance (Constitution) at its Article 40 guarantees the privacy of telegraphic and postal communications, and prohibits confiscation of communication. Further, Article 37 of the Basic Law of Governance provides that houses are inviolable; thereby, setting the ground for respect of privacy of individuals.

The Anti-Cyber Crime Law 2007, issued by Royal Decree No. M/17 on 8 Rabi'ul 1428H (26 March 2007), criminalises invasion of privacy and illegal and unauthorised use, access and modification of data, which includes, but is not limited to, the spying or illegal interception or reception of data transmitted through an information network or a computer. It also criminalises the unlawful access to computers with the motive of blackmailing or threatening any person.

1.3 Is there any sector-specific legislation that impacts data protection?

The following are sector-specific laws relating to data protection:

- The Telecommunication and Information Technology Act.
- The Electronic Commerce Law.
- The Electronic Transactions Law.
- The Law of Practicing Healthcare Professions.

- The Payment Service Provider Regulatory Guidelines issued by the Saudi Central Bank (SAMA).

1.4 What authority(ies) are responsible for data protection?

The Saudi Data and Artificial Intelligence Authority (SDAIA) is the competent authority to supervise the implementation of the provisions of the PDPL. The SDAIA, while exhausting its duties, can request the necessary information and documents from the Controller to ensure compliance with the PDPL and can request cooperation from other parties as well.

The National Cyber Security Authority has also been established to oversee Cyber Security in the Kingdom.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **“Personal Data”**
Any data, regardless of its source or form, that may lead to identifying an individual specifically, or that may directly or indirectly make it possible to identify an individual, including name, personal identification number, addresses, contact numbers, licence numbers, records, personal assets, bank and credit card numbers, photos and videos of an individual, and any other data of a personal nature.
- **“Processing”**
Any operation carried out on personal data by any means, whether manual or automated, including collecting, recording, saving, indexing, organising, formatting, storing, modifying, updating, consolidating, retrieving, using, disclosing, transmitting, publishing, sharing, linking, blocking, erasing and destroying data.
- **“Controller”**
Any public entity, natural person or private legal person that specifies the purpose and manner of processing personal data, whether the data is processed by that Controller or by the Processor.
- **“Processor”**
Any public entity, natural person or private legal person that processes personal data for the benefit and on behalf of the Controller.
- **“Data Subject”**
The individual to whom the personal data relate.

- **“Sensitive Personal Data”/“Special Categories of Personal Data”**
Personal data revealing racial or ethnic origin, or religious, intellectual or political belief; data relating to security, criminal convictions and offences, biometric or genetic data for the purpose of identifying the person; health data; and data that indicates that one or both of the individual’s parents are unknown.
- **“Data Breach”**
Any incident that leads to the disclosure, destruction or unauthorised access to personal data, whether intentional or accidental, and by any means, whether automated or manual.
- **“Pseudonymisation”**
Conversion of the main identifiers that indicate the identity of the data subject into codes that make it difficult to directly identify them without using additional data or information. The pseudonymised data or additional information should be kept separately, and appropriate technical and administrative controls should be implemented to ensure that they are not specifically linked to the data subject’s identity.
- **“Anonymisation”**
Removal of direct and indirect identifiers that indicate the identity of the data subject in a way that permanently makes it impossible to identify the data subject.
- **“Vital Interest”**
Any interest necessary to preserve the life of a data subject.

3 Territorial and Material Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The PDPL is applicable to any business established in other jurisdictions only if such business is, by any means, processing personal data of individuals residing in the Kingdom; this also includes the personal data of the deceased that would lead to the identification of such deceased individual or specifically their family.

3.2 Do the data protection laws in your jurisdiction carve out certain processing activities from their material scope?

The PDPL will not be applicable to processing that involves the processing of personal data for personal and family usage and does not go beyond it; however, such exemption is applicable only to the extent that the data subject does not publish his/her personal data to third parties. Personal and family use is defined as follows:

- Processing personal data, by individuals, within their family or limited social circle as part of any social or family activity. However, the following is excluded from the domain of personal or family use:
- When the personal data is published to the public or is disclosed to any person outside the definition of personal or family use.
 - When personal data is being used for professional, commercial or non-profit purposes.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
According to the PDPL, the means and methods used for the processing of personal data must be direct, clear and secure, must not involve any deception and must not mislead or extort the data subject for the processing of personal data.
- **Lawful basis for processing**
The purpose for which personal data is collected must be legitimate and should not be against any legal provision.
- **Purpose limitation**
The personal data processed must be appropriate and limited to the purpose for which it is collected.
- **Data minimisation**
The Controller must collect the minimum amount of personal data that is necessary to achieve the purpose for which personal data is being processed.
- **Proportionality**
Personal data processed must be proportionate to the extent that is necessary for the purpose for which personal data is collected.
- **Retention**
When the personal data collected is no longer necessary for the purpose for which it was collected, the Controller must cease their collection without undue delay and destroy previously collected personal data at once. However, the Controller may retain the personal data after completion of the purpose of collection, when the personal data processed does not contain anything that may lead to specifically identifying the data subject. In addition, the Controller may also retain the personal data in the following cases:
 - When there exists a legal basis for retaining personal data for a specific period of time; however, such personal data must be destroyed once the time period lapses or when the purpose of collection is satisfied, whichever is longer.
 - When the personal data processed is relevant with a case that is *sub judice* before a judicial authority, in such circumstances the personal data can be retained; however, once the judicial procedures are concluded, the Controller must destroy the personal data.
- **Accuracy**
The personal data processed must be accurate, complete and relevant to the purpose for which it is collected.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of information**
The data subject has a right to be informed of the legal basis and purpose of the processing of personal data. The following information, before or at the time of collection of personal data, is to be given to the data subject:
 - The identity of the Controller, including contact details and details related to the channels developed by the Controller for the data subject to have communication regarding protection of personal data.

- Contact details of the Data Protection Officer (DPO), when appointed.
- The legal basis and a clear, specific and explicit purpose of the processing of personal data.
- The duration the personal data will be kept. In case determining the period of retention is not possible, the data subject is to be informed about the criteria used to determine the retention period.
- Rights available to the data subject and the procedure to exercise the rights.
- The procedure to withdraw consent.
- Whether it is mandatory or optional to collect/process the personal data.
- **Right of access to (copies of) data/information about processing**
The law has given this right to the data subject that he/she can request for the copy of their personal data processed in a readable and clear format, on request by the data subject or without request by the data subject through a channel provided by the Controller, enabling the data subject to have access to the personal data. While requesting access to and copies of the personal data, the data subject is subject to the following conditions:
 - Exercise of such right, i.e. to access personal data, should not have any adverse effect on the rights of others, such as intellectual property rights or trade secrets.
 - Personal data is to be provided in a commonly used electronic format and the data subject may ask for a printed copy if feasible.
 - While granting the data subject access to their personal data, the Controller must ensure that the data being disclosed does not involve any such data that identifies another individual.
- **Right to rectification of errors**
The data subject has the right to request correction, completion or updating of personal data. In this regard, the Controller may request required evidence to verify the request of the data subject. The evidence, so provided by the data subject, must be destroyed once the verification process is completed.
After the correction of the personal data, the Controller shall, without undue delay, notify the parties to whom the personal data was previously disclosed.
- **Right to deletion/right to be forgotten**
The data subject can request the destruction of the processed personal data. The Controller is under obligation to destroy personal data in the following circumstances:
 - When the data subject has made a request for the personal data to be destroyed.
 - When the personal data is no longer necessary for the purpose it was collected.
 - If the data subject withdraws his/her consent for the processing of the personal data and the consent is the sole legal basis for processing.
 - If it comes into the Controller's knowledge that personal data is being processed in a manner that violates the PDPL.
 While destroying personal data, the Controller must be considerate of the following:
 - The Controller must take appropriate measures to notify the other parties with whom the Controller had shared the data and must request for the personal data to be destroyed.

- The Controller must notify any individual with whom the personal data has been shared by any means about the destruction of the personal data by the Controller and will request for him/her to do the same.
- The Controller must destroy all copies of the personal data stored in the Controller's systems, including any backups, in accordance with the applicable regulatory requirements.
- **Right to object to processing/Right to restrict processing**
A data subject can request the Controller to restrict processing in case the data subject has contested authenticity of the personal data processed by the Controller, and request for its correction. Such restriction period must enable the Controller to have a time period during which the Controller must verify the accuracy of the personal data.
- **Right to withdraw consent**
The data subject has the right to withdraw their consent for the processing of their personal data at any time. The data subject is to inform the Controller of such withdrawal through any available means in accordance with the Regulations.
- **Right to object to marketing**
The data subject has the right to opt for not receiving marketing materials. When a Controller has to process personal data for direct marketing purposes, it must obtain consent from the data subject. Also, the Controller must devise a mechanism that enables the data subject to opt out of receiving marketing materials.
- **Right to complain to the relevant data protection authority(ies)**
The data subject may complain to the competent authority after becoming aware of any incident necessitating making a complaint. The complaint must be filed within a period not exceeding 90 days from the date when the matter has come into the data subject's knowledge.
- **Other key rights**
The PDPL, besides laying down the penalties for the Controllers/Processors with respect to the violation of the PDPL, also gives a right to the data subject to file for compensation. An individual that suffers damage as a result of any of the violations stated in the PDPL or regulations may apply before a competent court of law for proportionate compensation for the material or moral damage.

5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

There is no such right under the PDPL.

6 Children's Personal Data

6.1 What additional obligations apply to the processing of children's personal data?

The PDPL enables a legal guardian to act on behalf of a data subject that partially or fully lacks the legal capacity. The PDPL requires the legal guardian to act in the best interests of the data subject, which may be a child in this case and for this purpose the PDPL has entrusted the legal guardian with two of the following options:

- On behalf of the data subject, the legal guardian can exercise the rights granted to the data subject (child) under the PDPL.
- The legal guardian can give consent on behalf of the data subject (child) for the processing of the personal data; however, the obtaining of the consent of the legal guardian is conditional upon the measures to be put in place to verify the validity of guardianship of the legal guardian over the data subject.

While obtaining consent from the legal guardian on behalf of the data subject (child), the Controller must be cautious of the following:

- This process shall not cause any harm to the interest of the data subject.
- It shall enable the data subject to exercise their rights as per the PDPL.

7 Registration Formalities and Prior Approval

7.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

The PDPL, while providing powers of the competent authority (SDAIA), empowers the SDAIA to specify the appropriate tools and mechanism to monitor compliance of the Controllers with the PDPL. These tools and mechanism may also include maintenance of a national register of Controllers.

The SDAIA has issued the Rules Governing the National Register of Controllers within the Kingdom for registration in the referred national register, including which Controllers must be registered.

7.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

The information needed, regarding processing activities, is a general description of the applicable processing activities.

7.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

The registration of the Controllers will be made as per their legal status; if a Controller falls into one of the following categories, it will be under obligation to register itself with the national register of Controllers:

- The Controller is a public entity.
- The Controller's main activity is based on personal data processing.
- The Controller is involved in the processing of sensitive personal data.
- In case of the Controller being an individual, if he/she is involved in the processing of personal data for purposes exceeding personal or family use.

7.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

As discussed in question 7.3.

7.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

In order to register in the national register of Controllers, the Controllers firstly need to appoint the representatives. In case of a public entity, a representative must be appointed through the registration form made available by the SDAIA on the national data governance platform, whereas in case of a private entity, a representative must be appointed by an authorised person on the platform provided. In case of individual Controllers, the individuals are their own representatives and are not required to designate other people.

The representative must then complete the registration process on the platform; the representative must complete all the required fields, including the following:

- Controller entity data comprising the entity logo, official email and contact number, and headquarters.
- Representative data comprising the official email and contact information.
- Individuals must complete all the required fields on the platform, including the official email and contact number.

7.6 What are the sanctions for failure to register/notify where required?

As discussed in question 16.4.

7.7 What is the fee per registration/notification (if applicable)?

No such fee is designated at the time of writing.

7.8 How frequently must registrations/notifications be renewed (if applicable)?

The registration certificate shall be valid for a period of five years. The SDAIA must notify the Controller of the impending expiry of their registration certificate 30 days prior to the expiry date. After the expiry date, the Controller will be given access to the platform for a grace period of five days.

7.9 Is any prior approval required from the data protection regulator?

No such prior approval is required.

7.10 Can the registration/notification be completed online?

The registration in the national register of Controllers is to be

done online through the national data governance platform managed by the SDAIA.

7.11 Is there a publicly available list of completed registrations/notifications?

The SDAIA must allow the public to verify the registration of Controllers in the national register by making the registration certificate publicly available in the national registry. The public can review the registration certificate and verify its authenticity.

7.12 How long does a typical registration/notification process take?

There is no information available regarding the exact time required to complete the registration; however, the process is seamless to facilitate registration.

8 Appointment of a Data Protection Officer

8.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The appointment of the DPO is mandatory in the following circumstances:

- The Controller is a public entity and is involved in the processing of the personal data on a large scale.
- The primary activities of the Controller involve the carrying out of such processing operations that require regular and continuous monitoring of individuals on a large scale.
- The Controller's core activities consist of processing sensitive personal data.

8.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

There is no dedicated/specified penalty for failing to appoint a DPO. Such failure being a violation of the PDPL, general penalties like a warning or a maximum fine of up to Saudi Riyals 5 million may be imposed. In case of repetitive violation, the fine may be doubled.

8.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

The PDPL is silent on this matter.

8.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

The PDPL is silent on this matter. The competent authority (SDAIA) is to issue rules for the appointment of a DPO. It is likely that such matters will be dealt with/clarified in the rules to be issued.

8.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The DPO may be an official, an employee, an external service provider of the Controller, or the Controller may also appoint its representative for registration as a DPO. The PDPL does not mention any specific qualification for the DPO. The competent authority (SDAIA) is to issue rules for the appointment of a DPO. It is likely that such matters will be dealt with/clarified in the rules to be issued.

8.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

Broadly, the DPO must monitor the implementation of the provisions of the PDPL and oversee the methods adopted by the Controller in order to comply with the PDPL and manage data subject requests.

The specific functions of the DPO include:

- To act as a point of contact between the competent authority and the Controller and to comply with the competent authority's decisions and instructions with respect to the application of the PDPL and its regulations.
- To supervise the following procedures and issue necessary recommendations accordingly:
 - i) impact assessments;
 - ii) audit reports;
 - iii) evaluations related to personal data protection controls; and
 - iv) documentation of assessment results.
- To enable the data subjects to exercise their rights as given under the PDPL.
- To notify the competent authority with respect to any incident of a personal data breach.
- To respond to requests made by data subjects and also to address complaints submitted by data subjects.
- To maintain and update the record of the processing activities of the Controller.
- To address any violations of the PDPL made by the Controller and to take the corrective measures.

8.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

When a Controller appoints a DPO, the representative of the Controller will be under obligation to fill in the DPO's information on the platform provided by the authority to create the Controller's account.

In case the DPO is an employee of the Controller or an external contractor, the representative must provide the following information:

- a) The DPO's national ID/residency number for data retrieval purposes.
- b) The DPO's date of birth for verification of the entered national ID/residency number.
- c) The DPO's official contact information (phone number and email).

Where the DPO is a contractor located outside the Kingdom, the following information must be provided:

- a) First and last name.
- b) Official email address.
- c) Official contact number.

8.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

As part of the rights conferred on the data subjects (right to be informed), the Controller must inform the data subjects of the DPO's contact details.

9 Appointment of Processors

9.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

While appointing the Processor for the processing on behalf of the Controller, the Controller must ensure that the appointed Processor provides sufficient guarantees to comply with the PDPL and its implementing regulations. The Controller, in this regard, must conclude an agreement with the Processor. Such guarantees, however, do not dilute the obligations of the Controller towards the data subject or the competent authority.

9.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

It is necessary to enter into an agreement with the Processor. The agreement must provide the following:

- a) The purpose for which the personal data is to be processed.
- b) The categories of the personal data being processed.
- c) The duration for which the processing will take place.
- d) The Processor's commitment to notify the Controller of any breach incident, in accordance with the provisions of the PDPL.
- e) Clarification from the Processor that similar laws (equivalent to the PDPL) in other jurisdictions are applicable on its impact on the processing.
- f) That the Processor need not obtain the data subject's prior consent for mandatory disclosure of personal data under the applicable laws in the Kingdom; however, the Processor must notify the Controller of any such disclosure.
- g) The Processor shall identify any sub-contractors to be appointed by the Processor, or any other party with whom the personal data shall be shared.

10 Marketing

10.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

Public entities may use personal means of communication (post and email) for sending awareness-raising material. However, the Controller may not use personal means of communication, including post and email, unless it fulfils certain conditions. Before sending awareness-raising material, the Controller must:

- obtain the consent of the recipient; and

- provide a clear mechanism to enable the recipient to opt out of receiving such awareness-raising material.

In addition to the applicable requirements under the Telecommunication and Information Technology Act, the Controller is further to observe the following:

- To clearly show the identity of the sender.
- To provide a mechanism enabling the data subject to opt out and to ensure that the relevant procedure to opt out is as easy as to give consent.
- To immediately stop sending materials as soon as the recipient asks to opt out.
- To stop sending the material without any fee.
- To preserve the consent received from the recipient.

Apart from the above, the Controller (with the exception of sensitive data) may process personal data for marketing purposes by observing the following controls:

- Obtaining the consent of the data subject.
- Providing a mechanism enabling the data subject to opt out and to ensure that the relevant procedure to opt out is as easy as to give consent.
- Clearly state the identity of the sender without any anonymisation.
- Immediately stop sending marketing materials as soon as the data subject withdraws his/her consent.

10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

The PDPL does not draw any differentiation, in the context of business-to-consumer or business-to-business marketing, as regards the above-mentioned controls.

10.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

As explained at question 10.1 above.

10.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?

As the PDPL is applicable to Controllers outside the Kingdom (due to extra-territorial applicability), the controls mentioned above do apply to marketing sent from other jurisdictions.

10.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

At the time of writing, no enforcement actions are publicly known.

10.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

The PDPL is silent on this matter; however, this seems against the very principles of the PDPL unless consented by the data subjects.

10.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

There is no dedicated/specified penalty for sending marketing communications in contradiction of the requirements of the PDPL. Such contradiction being violation of the PDPL, general penalties like a warning or a maximum fine of up to Saudi Riyals 5 million may be imposed. In case of repetitive violation, the fine may be doubled. In case sensitive data is the subject matter of any marketing, the maximum penalty is Saudi Riyals 3 million or imprisonment for up to two years, or both.

11 Cookies

11.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

The PDPL is silent on the use of cookies.

11.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

The PDPL is silent on the use of cookies.

11.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

The PDPL is silent on the use of cookies.

11.4 What are the maximum penalties for breaches of applicable cookie restrictions?

The PDPL is silent on the use of cookies.

12 Restrictions on International Data Transfers

12.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

A Controller may transfer personal data outside the Kingdom or may disclose it to a party outside the Kingdom in order to achieve the following purposes:

- If the data to be transferred is related to performing an obligation under an agreement to which the Kingdom is party.
- If such transfer of personal data would serve the interest of the Kingdom.
- If the transfer of the personal data is with respect to the performance of an obligation.
- If the transfer is for the purposes as mentioned in the regulations (Regulation on Personal Data Transfer outside the Kingdom).

Conditions to be met for the transfer of personal data

While transferring personal data outside the Kingdom, the Controller must consider the following conditions:

- The transfer or disclosure of personal data must not cause any prejudice to national security or vital interests of the Kingdom or violate any other law of the Kingdom.

- The Controller must limit the transfer or disclosure of the personal data outside the Kingdom, i.e. only the minimum data must be transferred that is necessary to achieve the purpose of the disclosure/transfer.
- The Controller must ensure there is an adequate level of protection for personal data outside the Kingdom. There must be at least similar protection, outside the Kingdom, as is available under the PDPL in accordance with the assessment carried out by the competent authority.

While transferring personal data outside the Kingdom, the Controller must ensure that the disclosure/transfer does not impact the privacy of the data subjects or does not impact negatively the level of protection guaranteed under the PDPL. Considering these points, the Controller must ensure that the following aspects are not compromised:

- The data subject's ability to exercise their rights as conferred by the PDPL.
- The data subject's ability to exercise their right to withdraw their consent to the processing.
- The Controller's ability to comply with requirements for notifying personal data breaches.
- The Controller's ability to comply with provisions, controls and procedures for disclosing personal data.
- The Controller's ability to comply with provisions and controls for destroying personal data.
- The Controller's ability to take necessary organisational, administrative and technical measures to ensure the security of the personal data.

In the absence of an adequate level of protection, the personal data may be transferred by way of the following appropriate safeguards:

- Binding Common Rules (as approved by the competent authority).
- Standard Contractual Clauses (as issued by the competent authority).
- Certification of Compliance by an entity authorised by the competent authority.
- Binding Codes of Conduct (as approved by the competent authority).

12.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

At the time of writing, the SDAIA has not issued a list of adequate jurisdictions; however, the SDAIA has issued model Standard Contractual Clauses and Binding Common Rules for the guidance of businesses regarding cross-border transfer of personal data.

12.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

As mentioned at question 12.1, the Binding Common Rules, Standard Contractual Clauses and Binding Codes of Conduct must be issued/approved by the competent authority.

12.4 Do transfers of personal data to other jurisdictions require a transfer impact assessment? If conducting a transfer impact assessment is only mandatory in some circumstances, please identify those circumstances.

The Controller must conduct a risk assessment for the transfer of personal data outside the Kingdom or disclosure to a party outside the Kingdom in any of the following cases:

- When the transfer of the personal data outside the Kingdom is based on appropriate safeguards.
- When the appropriate safeguards for transfer of personal data outside the Kingdom are not required.
- When continuous or large-scale transfer of sensitive personal data is to be carried out outside the Kingdom.

12.5 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?

This is not applicable.

12.6 What guidance (if any) has/have the data protection authority(ies) issued in relation to the use of standard contractual/model clauses as a mechanism for international data transfers?

The SDAIA has issued guidelines for Standard Contractual Clauses. The following four templates have been issued by the SDAIA:

- First template: governs the transfer of personal data outside the Kingdom from Controller to Controller.
- Second template: governs the transfer of personal data outside the Kingdom from Controller to Processor.
- Third template: governs the transfer of personal data outside the Kingdom from Processor to Processor.
- Fourth template: governs the transfer of personal data outside the Kingdom from Processor to Controller.

13 Whistle-blower Hotlines

13.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

On 13 February 2024, a new law for the Protection of Whistle blowers, Witnesses, Experts and Victims was published. The said law provides for the court to protect individuals who give evidence from being intimidated that may cause impact on their testimony, including whistleblowers, other witnesses, experts and victims. Protection includes removing their name and address from any correspondence, documents and minutes, concealing them while giving evidence in court or permitting them to give evidence behind closed doors. Based upon the said law, the establishment of the Centre for the Protection of Whistleblowers, Witnesses, Experts and Victims has also been approved.

13.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous reporting is generally permitted.

14 CCTV

14.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

A law relating to the use of surveillance cameras in the Kingdom is made *vide* Royal Decree No. 164 dated 7 October 2022 (the KSA Surveillance Cameras Law). The KSA Surveillance Cameras Law makes it mandatory to install surveillance cameras in public places like ministries, commercial complexes, health care facilities, financial institutions, etc. The KSA Surveillance Cameras Law states that installing, operating or maintaining security surveillance cameras is not permissible except with the approval of the Ministry of Interior.

14.2 Are there limits on the purposes for which CCTV data may be used?

As mentioned at question 14.1.

15 Employee Monitoring

15.1 What types of employee monitoring are permitted (if any), and in what circumstances?

The PDPL is silent on employee monitoring.

15.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

The PDPL does not create any exception as regards the processing of personal data of employees or otherwise. Therefore, consent is required unless specifically excluded. The most typical mode to obtain consent from employees is through an employment agreement.

15.3 To what extent do works councils/trade unions/ employee representatives need to be notified or consulted?

Trade unions are not permitted in the Kingdom.

15.4 Are employers entitled to process information on an employee's attendance in office (e.g., to monitor compliance with any internal return-to-office policies)?

There is no specific restriction to process an employee's attendance in office.

16 Data Security and Data Breach

16.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

The Controller shall take the necessary organisational, administrative and technical measures to ensure the security of personal data and the privacy of data subjects. For security purposes, the Controller must comply with the following:

- Implement necessary security and technical measures to limit security risks related to a personal data breach.
- Comply with the relevant controls, standards and rules issued by the National Cybersecurity Authority or recognised best practices and cyber security standards if the Controller is not obligated to follow the controls, standard and rules issued by the National Cybersecurity Authority.

The Controller, while appointing a Processor, shall ensure that the chosen Processor provides sufficient guarantees to protect the personal data.

16.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

When a data breach incident will potentially cause harm to the personal data or to the data subject, or conflicts with the data subject's rights and interests, the Controller shall notify the authority within a time period not exceeding 72 hours of becoming aware of the incident. If the Controller fails to notify the authority within the prescribed time after it became aware of the breach incident, then it shall provide the requisite information to the authority as soon as possible, along with a justification of delay. The Controller must also keep a copy of the report submitted to the authority and must document the corrective measures taken in relation with the personal data breach, as well as any relevant documents or supporting evidence.

The data breach notification shall include the following information:

- a) A description of the personal data breach incident, which includes the time, date and circumstances of the breach and the time when the Controller became aware of the breach.
- b) The categories of data impacted by the breach, actual or approximate numbers of impacted data subjects and the type of personal data effected by the breach incident.
- c) A description of the risks of the personal data breach, including the actual or potential impact on personal data and data subjects, and the actions and measures taken by the Controller after the breach to prevent or limit the impact of those risks and to mitigate these risks. Also a description of the future measures that will be taken to avoid a recurrence of the breach.
- d) A statement of the Controller wherein it states whether the data subject has been notified of the breach incident.
- e) Contact details of the Controller or any DPO, if appointed, or any other official who has knowledge of the reported incident.

The provisions of the PDPL do not prejudice the obligations of the Controller or Processor as conferred by the National Cybersecurity Authority, relevant to the personal data breach notification.

16.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

When an incident of personal data breach may cause damage to the data subject's personal data or may conflict with their rights or interests, the Controller must notify the data subject of such incident of breach without undue delay (i.e. within 72 hours); furthermore, the language of the notification must be simple and clear. The personal data breach to be notified to the data subject must include the following information:

- A description of the personal data breach.
- A description of the potential risks that may arise from the personal data breach.
- A description of the measures taken to mitigate the potential risks that may arise from the personal data breach.
- The name and contact details of the Controller, as well as the contact details of any DPO appointed; moreover, any appropriate means of communication with the Controller.
- The notification shall contain a recommendation or advice that may assist the data subject in taking appropriate measures to safeguard against the identified risks or to mitigate the impact of the potential risks.

16.4 What are the maximum penalties for personal data security breaches?

Any individual who violates the provisions of the PDPL by disclosing or publishing sensitive personal data, with the intention of harming the data subject or achieving any personal motive, shall be punished with an imprisonment for a period not exceeding two years or a fine not exceeding Saudi Riyals 3 million, or both.

Apart from the above, any other violation of the PDPL attracts the issuance of a warning, or a maximum fine of up to Saudi Riyals 5 million may be imposed. In case of repetitive violation, the fine may be doubled.

17 Enforcement and Sanctions

17.1 Describe the enforcement powers of the data protection authority(ies).

- a) **Implementation:** The SDAIA, being the competent authority, has the mandate to oversee the implementation of the PDPL and its implementing regulations.
- b) **Calling for Documents or Information:** The SDAIA is empowered to ask the Controllers for the necessary documents or information to ensure compliance of the PDPL.
- c) **Asking Cooperation:** The SDAIA may request any party to cooperate to support the accomplishment of its enforcement functions under the PDPL.

- d) **Specification of Tools:** The SDAIA may, in order to monitor compliance by the Controllers, specify the appropriate tools and mechanism, including maintaining a national register of Controllers.
- e) **Service Provision:** The SDAIA may, through the referred national register, provide services related to personal data protection.
- f) **Complaints Processing:** The SDAIA is empowered to receive and to take actions on the complaints of the data subjects.

17.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

This power is not mentioned in the PDPL.

17.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

No public information is available.

17.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

No public information is available.

18 E-discovery/Disclosure to Foreign Law Enforcement Agencies

18.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

The PDPL is silent on this aspect. However, generally, the foreign law enforcement agencies do not communicate with businesses directly; rather, businesses are contacted via the relevant law enforcement agencies of the Kingdom, who coordinate with businesses to respond to foreign law enforcement agencies.

18.2 What guidance has/have the data protection authority(ies) issued on disclosure of personal data to foreign law enforcement or governmental bodies?

No guidance has been issued.

19 Artificial Intelligence

19.1 Are there any limitations on automated decision-making involving the processing of personal data using artificial intelligence?

The PDPL requires explicit consent for the processing of personal data when carried out through automated means and decisions are made solely based on automated processing of personal data.

19.2 What guidance (if any) has/have the data protection authority(ies) issued in relation to the processing of personal data in connection with artificial intelligence?

The SDAIA has issued the Artificial Intelligence (AI) Ethics Principles, which not only define AI but also set out the principles that are to be followed by entities while using AI.

As per the AI Ethics Principles, AI is defined as “a collection of technologies that can enable a machine or system to sense, comprehend, act, and learn”.

The following principles are to be followed while using AI:

- 1. Fairness.
- 2. Privacy and security.
- 3. Humanity.
- 4. Social and environmental benefits.
- 5. Reliability and safety.
- 6. Transparency and explainability.
- 7. Accountability and responsibility.

20 Trends and Developments

20.1 In your opinion, what enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.

The SDAIA has designated the Saudi Central Bank with the responsibility of achieving compliance with the PDPL by the entities licensed by the central bank. This approach has resulted in making an effective compliance programme within the entities licensed by the Saudi Central Bank. Considering this, it may be anticipated that the SDAIA may mandate the Saudi Central Bank to have a compliance audit of the entities licensed by it.

20.2 In your opinion, what “hot topics” are currently a focus for the data protection regulator?

Data privacy in the newest and emerging technologies, in particular AI, seems to be of pertinent focus concerning the development of a regulatory framework.



Saifullah Khan is an international trade, privacy and policy lawyer with more than 20 years of diversified and multi-jurisdictional professional experience serving a large client base in the domestic and international markets. His areas of interest include trade remedy laws of the World Trade Organization, customs law, competition law and data privacy. With respect to emerging discipline of data privacy, he advises clients from different jurisdictions on data privacy compliance and cross-border transfer of data. Additionally, he assists clients in the preparation and review of privacy policies and intra-group agreements concerning cross-border transfer of personal data, etc. He is an advocate of the High Court, a member of the Chartered Institute of Arbitrators (UK) and a member of the International Association of Privacy Professionals. He has completed a course at the London School of Economics and Political Science on "Data: Law, Policy and Regulation".

Droua Al-Amal Consultants

7289-7207 Wadi Taraj
An Nakheel Riyadh 12381
Saudi Arabia

Tel: +966 53 069 2265
Email: saifullah.khan@drouaalamal.sa
LinkedIn: www.linkedin.com/in/saifullahkhan



Saeed Hasan Khan has vast experience advising clients on various issues such as taxation, corporate, regulatory compliance, contractual obligations, etc. and representing them before the authorities. Over the past 20 years, he has practised in direct and indirect taxes, which encompasses all three practice tiers: advisory; execution; and litigation. He advises on cross-border transactions, international tax treaties and matters related to tax due diligence, corporate structures, shareholder agreements and contractual stipulations between the companies. He has developed a keen professional interest in emerging laws about personal data protection and has gained a deep understanding of underlying concepts and principles governing the global data protection laws including the General Data Protection Regulation of the European Union.

He carried out a great deal of research on personal data protection laws in various jurisdictions to have a comparison of core legal principles in a range of jurisdictions. He attended a course at the London School of Economics and Political Science on "Data: Law, Policy and Regulation". He is an Advocate of the High Court, a Member of the Chartered Institute of Arbitrators (UK) and a Member of the International Association of Privacy Professionals.

Droua Al-Amal Consultants

7289-7207 Wadi Taraj
An Nakheel Riyadh 12381
Saudi Arabia

Tel: +966 53 906 2286
Email: saeed.hasan@drouaalamal.sa
LinkedIn: www.linkedin.com/in/saeedhasankhan

Droua Al-Amal Consultants carries the rich, multi-faceted and multi-jurisdictional experience, spreading over two decades, of its directors. The company endeavours to be a professional service provider, which synthesises the learning from a vast experience-base and converts that into advantage for its clients. The services we offer, to our prestigious clients, are based on profound industry and legal knowledge.

www.drouaalamal.sa

DROUA
شركة ذروة الاعمال للاستشارات المهنية
Droua Alamal For Consultancy Services

Serbia

Mikijelj Jankovic & Bogdanovic



Vladimir
Djerić



Lena
Petrovic



Katarina
Radovic



Kristina
Petronijevic

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The principal data protection legislation in Serbia is the Personal Data Protection Act (“*Official Gazette of the Republic of Serbia*”, no. 87/2018), which became effective on 21 August 2019 (**PDPA**). The PDPA is largely harmonised with the EU GDPR. However, it does not contain the recitals of the GDPR that provide guidance for better understanding and implementing of the GDPR. This, together with the lack of practice by courts, makes the PDPA more difficult to interpret.

1.2 Is there any other general legislation that impacts data protection?

In addition to the PDPA, the Constitution of Serbia contains several provisions relating to the protection of privacy, including the confidentiality of letters and other means of communication (Article 41 of the Constitution) and the protection of personal data (Article 42 of the Constitution).

Under the Constitution, the confidentiality of letters and other means of communication may only be derogated from for a specified period of time and based on a court decision for the purpose of conducting criminal proceedings or protecting the security of Serbia, in a manner stipulated by the law (Article 41 of the Constitution).

The Constitution of Serbia guarantees protection of personal data and states that the use of personal data for any purpose other than that for which they were collected in accordance with law is prohibited and punishable unless this is necessary to conduct criminal proceedings or protect the security of Serbia, in a manner stipulated by law. In addition, the Constitution also sets out the right of individuals to be informed of the collection of their personal data, in accordance with the law, as well as the right to court protection in the case of abuse of their personal data (Article 42 of the Constitution).

Furthermore, provisions that are of relevance to the protection of personal data may also be found in:

- The Electronic Communications Act (**ECA**) – governing the use of personal data in relation to direct marketing.
- The Information Security Act – governing cyber security matters.
- The Criminal Code.

1.3 Is there any sector-specific legislation that impacts data protection?

There are multiple sector-specific legislation that impact data protection, such as:

- The Employment Act.
- The Banking Act.
- The Trade Act.
- The Science and Research Act.
- The Protection of Users of Financial Services Act.
- The Advertising Act.
- The Consumer Protection Act.

1.4 What authority(ies) are responsible for data protection?

The main authority is the Commissioner for information of public importance and personal data protection (**Commissioner**). Additionally, misdemeanour courts and administrative courts are in charge if a case is brought before the court, i.e. if an affected party initiates administrative court proceedings against the decisions of the Commissioner or if the Commissioner initiates misdemeanour proceedings regarding violation of the PDPA.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **“Personal Data”**
Any information relating to an identified or identifiable natural person (i.e. a data subject), directly or indirectly, in particular by reference to an identifier such as a name and an identification number, location data, an online identifier in electronic communication networks or to one and/or more characteristics of the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- **“Processing”**
Any operation or set of operations that is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, classification, grouping and/or structuring, storage, adaptation or alteration, disclosure, consultation, use, disclosure by transmission and/or by delivery, propagation, dissemination or otherwise making available, comparison, restriction, erasure or destruction.

- **“Controller”**
Natural or legal person or public authority that, alone or jointly with others, determines the purpose and means of the processing. The law determining the purpose and means of processing may provide for the controller or the specific criteria for its nomination.
- **“Processor”**
A natural or legal person, or public authority that processes personal data on behalf of the controller.
- **“Data Subject”**
A natural person whose personal data are processed.
- **“Sensitive Personal Data”/“Special Categories of Personal Data”**
Personal data on racial or ethnic origin, political opinion, religious or philosophical belief, or trade union membership genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.
- **“Data Breach”**
A breach of security of personal data leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
- **“Profiling”**
Any form of automated processing used to evaluate certain personal aspects relating to a natural person, in particular with the aim to analyse or predict that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
- **“Pseudonymisation”**
Processing in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical, organisational and personnel-related measures to ensure that the personal data cannot be attributed to an identified or identifiable person.
- **“Consent”**
Consent of the data subject means any freely given, specific, informed and unambiguous expression of the data subject’s wishes by which such person, by a statement or by a clear affirmative action, agrees to the processing of personal data relating to him or her.
- **“Genetic Data”**
Personal data relating to the inherited or acquired genetic characteristics of a natural person that give unique information about the physiology or the health of such person and that result, in particular, from an analysis of a biological sample.
- **“Biometric Data”**
Personal data resulting from specific technical processing relating to physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that person, such as facial images of dactyloscopic data.
- **“Data Concerning Health”**
Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

3 Territorial and Material Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

Yes, the PDPA applies to:

- i) The processing of personal data in the context of the activities on the territory of Serbia by a controller or a processor established in Serbia, whether or not the processing takes place in Serbia.
- ii) The processing of personal data of individuals who are in Serbia by a controller or processor not established in Serbia, where the processing activities are related to: (a) the offering of goods or services to individuals in Serbia (irrespective of whether a payment is required); or (b) the monitoring of an individual’s behaviour, where that behaviour takes place within Serbia.

To be considered “established” in Serbia, the following conditions must be met:

- For a natural person – they must have residence or temporary residence in Serbia.
- For companies – they must have a seat, i.e. an establishment, in Serbia.

3.2 Do the data protection laws in your jurisdiction carve out certain processing activities from their material scope?

Yes, the PDPA does not apply to the processing of personal data by a natural person in the course of a personal or household activity.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
Data should be processed in a transparent manner in relation to the data subject.
- **Lawful basis for processing**
Lawful processing is processing done in accordance with the law.
- **Purpose limitation**
Personal data is collected for specified, explicit, justified and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- **Data minimisation**
Processing shall be adequate, relevant and limited to what is necessary in relation to the purposes for which data is processed.
- **Proportionality**
Processing should be limited to the minimum necessary to achieve the intended purpose, i.e. there should be a balance between data processing and impact to protection of privacy of individuals.
- **Retention**
Data should be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes of processing (**storage limitation**).
- **Accuracy**
Personal data shall be accurate and, where necessary, kept up to date. Having regard to the purposes for which

they are processed, every reasonable step must be taken to ensure that inaccurate personal data are erased or rectified without delay.

- **Integrity and confidentiality**
Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical, organisational and personnel-related measures.
- **Accountability**
The controller is responsible for, and should be able to demonstrate compliance with, the principles relating to processing of personal data.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to (copies of) data/information about processing**
The data subject shall have the right to request from the controller confirmation as to whether personal data concerning him or her are being processed, access to such data and the information about the purpose of the processing, the categories of personal data concerned, the recipient to whom the personal data have been or will be disclosed, the envisaged period for which the personal data will be stored and other information related to the data subject right prescribed by the PDPA.
- **Right to rectification of errors**
The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her.
- **Right to deletion/right to be forgotten**
The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her.
- **Right to object to processing**
The controller shall no longer process the personal data of the data subject who has objected unless it demonstrates compelling legitimate grounds for the processing that override the interests, rights and freedoms of the data subject or for the filing, exercise or defence of legal claims.
- **Right to restrict processing**
The data subject shall have the right to obtain from the controller restriction of processing of his or her personal data where one of the following applies:
 - 1) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
 - 2) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
 - 3) the controller no longer needs the personal data for the purpose of the processing, but they are required by the data subjects for the establishment, exercise or defence of legal claims; or
 - 4) the data subject has objected to processing pending the verification whether the legal grounds for processing by the controller override the interests of the data subject.
- **Right to data portability**
The data subject shall have the right to receive his or her personal data, which he or she has previously provided to a controller, in a structured, commonly used and

machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided where the processing is based on consent or on a contract and where the processing is carried out by automated means.

- **Right to withdraw consent**
The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed of the right to withdraw and the effect of withdrawal.
- **Right to object to marketing**
Where personal data is processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.
- **Right protecting against solely automated decision-making and profiling**
The PDPA provides that the data subject has the right to object if:
 - i) an automated decision is based solely on automated processing (including profiling) – this means that there is no human involvement in the decision-making process; and
 - ii) an automated decision produces legal effects for an individual, or otherwise significantly affects an individual.

The aforementioned does not apply if the decision is:

 - a) necessary for entering into, or performing, a contract between the individual and the controller;
 - b) required or authorised by Serbian law, which also sets suitable safeguards for protection of rights and interests of the individual; or
 - c) based on the individual's explicit consent.

Under the PDPA, if the significant automated decision is permitted because it is necessary for a contract or based on the individual's consent, the controller must give the individual the right to request human intervention by the controller, to express their point of view, to obtain an explanation of the decision and to contest the decision. The controller must also implement other appropriate measures to safeguard the interests of the individual. Under the PDPA, if the significant automated decision involves special types of personal data, it may only take place if the individual has also given explicit consent, clearly made the data being processed publicly available, or the processing is necessary for reasons of substantial public interest, and the controller has suitable measures in place to safeguard the interests of the individual.
- **Right to complain to the relevant data protection authority(ies)**
The data subject is authorised to lodge a complaint to the Commissioner if he or she considers that there is a violation of the PDPA with respect to the processing of his or her personal data.

5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

Under the PDPA, the data subject has the right to authorise

a representative of an association active in the field of the protection of the data subject's rights and freedoms with regard to the protection of their personal data. A collective redress mechanism is not available.

6 Children's Personal Data

6.1 What additional obligations apply to the processing of children's personal data?

Generally, consent for data processing is valid if it is given by a person of 18 years of age or older. The PDPA recognises exceptions to this rule in relation to consent concerning Online Services. Under the PDPA, 15-year-old persons are able to give consent in relation to Online Services. On behalf of persons younger than 15, consent is given by their parents or other personal representatives of a minor.

7 Registration Formalities and Prior Approval

7.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

No, there is no such obligation under the PDPA.

7.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

This is not applicable.

7.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

This is not applicable.

7.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

This is not applicable.

7.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

This is not applicable.

7.6 What are the sanctions for failure to register/notify where required?

This is not applicable.

7.7 What is the fee per registration/notification (if applicable)?

This is not applicable.

7.8 How frequently must registrations/notifications be renewed (if applicable)?

This is not applicable.

7.9 Is any prior approval required from the data protection regulator?

This is not applicable.

7.10 Can the registration/notification be completed online?

This is not applicable.

7.11 Is there a publicly available list of completed registrations/notifications?

This is not applicable.

7.12 How long does a typical registration/notification process take?

This is not applicable.

8 Appointment of a Data Protection Officer

8.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

Under the PDPA there is no general requirement for all organisations to appoint a Data Protection Officer (DPO), but controllers and processors must appoint a DPO: (i) if they are a public authority or body (excluding courts acting in a judicial capacity); or (ii) where the core activities of the controller or processor consist of:

- a) processing activities that, by their nature, scope or purposes, require regular and systematic supervision of a large number of data subjects; or
- b) processing on a large scale of special types of personal data or criminal offence data.

8.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

If the controller or processor does not designate a DPO when required to do so (i.e. as outlined above under question 8.1), it will be fined for the offence in the range of RSD 50,000–2 million.

8.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

Yes, he or she is protected.

8.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

Under the PDPA, a group of organisations (under common control) may appoint a single DPO, provided that the DPO is easily accessible from each place of business.

The concept of availability refers primarily to the possibility of adequately performing the tasks, as a point of contact, both within the organisation itself and for the persons whose data is in question, as well as for the supervisory body. The term “group companies”, in the sense of the provisions of Article 4, point 20 of the PDPA, means a group of related economic entities, in accordance with the Companies Act. Therefore, when appointing a DPO in each specific case, it must be taken into account that the DPO must be able to effectively perform the tasks established by the provisions of the PDPA, as well as any other obligations established by special laws that can be applied, depending on the circumstances in each specific case.

In order for a DPO to be easily accessible, their contact details should be readily available to employees, the Commissioner and to individuals.

There is no specific requirement under the PDPA for the DPO to be in Serbia.

8.5 Please describe any specific qualifications for the Data Protection Officer required by law.

Under the PDPA, the DPO must be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks assigned to the DPO. There are no specific qualifications imposed by the law.

8.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

Under the PDPA, the responsibilities of a DPO are to:

- inform and advise the controller or processor and any employees who carry out processing of personal data of their legal obligations that are the protection of personal data;
- monitor compliance by the organisation with the PDPA, other Serbian data protection laws and the policies of the organisation in relation to the protection of personal data, including assignment of responsibilities, awareness-raising and training of relevant staff, and the related audits;
- where requested, advise on and monitor the performance of Data Protection Impact Assessments (DPIAs); and
- cooperate and consult with the Commissioner, and act as the contact point for the Commissioner on issues relating to processing, including prior consultation where required on a DPIA.

8.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

Yes, to the Commissioner.

8.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

Under the PDPA, the organisation must publish the contact details of the DPO and communicate them to the Commissioner. Failure to do so is a punishable offence, subject to a fine of RSD 100,000.

9 Appointment of Processors

9.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes, the agreement or some other form of legally binding document between the controller and the processor should be concluded in writing.

9.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

Processing by a processor shall be governed by a contract or other legally binding act that is concluded or adopted in writing, including in electronic form, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, and the obligations and rights of the controller.

Such contract or other legally binding act shall provide that the processor:

- 1) processes the personal data only on the basis of documented instructions from the controller;
- 2) ensures that natural persons authorised to process the personal data have committed themselves to confidentiality or are under appropriate statutory obligation of confidentiality;
- 3) takes all measures for safe and secure data processing;
- 4) respects the conditions for engaging another processor;
- 5) assists the controller by appropriate technical, organisational and personnel-related measures, insofar as this is possible, for the fulfilment of the controller’s obligations to respond to requests for exercising the data subject’s rights;
- 6) assists the controller in ensuring compliance with the legal obligations;
- 7) after the performance of the agreed processing, and upon the decision of the controller, deletes or returns all the personal data to the controller, and deletes all existing copies of such data, unless the law requires storage of the personal data; and
- 8) makes available to the controller all information necessary to demonstrate compliance with the obligations of the processor provided in this chapter and information that allow for and contribute to the inspection of the processor’s work, conducted by the controller or another person authorised by the controller.

10 Marketing

10.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

Under the Advertising Act (Article 63) and the ECA (Article 8), direct electronic marketing sent to an individual, who is a natural person, requires consent from the recipient.

The necessary form of the individual's consent is not specified in the Advertising Act, but it is recommended to have some evidence of an individual's consent, such as a record of visitation of the web page or similar. However, under the PDPA, the use of a pre-ticked box is not a valid way of obtaining consent. Consent can be revoked at any time, and the advertiser, that is, the transmitter of the advertising message, must enable this revocation.

If the individual has expressly agreed to advertising by telephone, fax, email or other means of distance communication, the trader is obliged to inform the individual about the commercial purpose of the activity in a clear and unambiguous manner, in the Serbian language, before advertising a certain good or service.

Should the individual object to direct advertising, the advertiser, that is, the transmitter of the advertising message, is obliged to stop such type of advertising in the future.

10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

Under the Advertising Act, consent is not required when a marketing communication is sent to persons performing professional or business activities, in connection with that activity (business communication). However, under the Electronic Commerce Act, sending electronically a marketing communication concerning information society services requires consent of the recipient, be it an individual or businessperson.

In any case, consent is not required where the communication is sent to a general business email address (this would not fall within the definition of personal data and consequently a lawful basis under the PDPA is not required either).

10.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

The Consumer Protection Act prescribes that direct advertising by telephone without the prior consent of the consumer is prohibited. It is also prohibited to call or send messages by telephone to consumers whose telephone numbers are registered in the register of consumers who do not want to receive calls and/or messages within the framework of promotion and/or sales by telephone. The Ministry of Internal and Foreign Trade has stated that, in accordance with the Consumer Protection Act and in order to protect vulnerable groups of consumers as effectively as possible, the "Do Not Call" register started operating from January 5, 2024. Consumers who do not want to receive calls from traders via phone and text messages for the purpose of selling products or services can be

registered in this register, and all mobile and fixed telephony controllers are obliged to enable this for their users.

This register is maintained by the regulatory body responsible for electronic communications and contains the consumer's first and last name, the consumer's personal identity number, telephone number and the date of entry into the register. The register will be public in the part that refers to telephone numbers and the date of entry into the register. Regardless of the entry in the register, the consumer's consent for direct advertising given to the trader before or after the entry in the register is valid until its revocation, which is given in accordance with the PDPA.

10.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?

In principle yes, all legal entities conducting their marketing activities aimed at Serbian citizens should comply with the Serbian legislation. However, it is possible to assume that certain unlawful marketing activity of a company seated outside Serbia might not be sanctioned due to complex and long procedures for international legal cooperation between the states in accordance with the applicable instruments of international public law (convention on legal cooperation, bilateral state agreements and alike).

10.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

We are not aware of any activities of the Commissioner with respect to breaches of marketing restrictions. Other regulatory bodies and inspectors who monitor application of the Consumer Protection Act and Advertising Act are more focused on the sanctioning of unlawful marketing activities.

10.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

There is no prohibition on purchase of marketing lists from third parties. However, it is the organisation undertaking the marketing, as controller, (and not the selling entity) who will be responsible for the personal data it holds (including how that data was acquired), and how it is used. The organisation (as controller) is responsible for the contact details it holds (including how they were acquired) and the marketing communications it sends.

An organisation should complete due diligence to satisfy itself that the marketing list was collected fairly, transparently and with a valid lawful basis, e.g. that consent is valid and recent enough to cover the intended marketing. Bought-in lists can only be used for sending marketing texts or emails if the individuals on the list specifically consented to receive that type of message from that organisation – generic consent covering any third party or category is not sufficient.

It is prudent for an organisation to have a written contract in place with the third party confirming the reliability of the personal data, giving reasonable control and audit powers and ideally including an indemnity for any breach of the relevant laws. Ultimately, if a third party cannot provide reassurance regarding the reliability/validity of a marketing list for the intended purpose, or if their explanations are not satisfactory, an organisation should not use it.

10.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Under the Advertising Act, a fine between RSD 300,000 and 2 million will be issued by the Misdemeanour Court to the legal entity who performs (i.e. is responsible for) direct marketing contrary to provisions of the Advertising Act.

Under the PDPA, a fine in the amount of RSD 100,000 shall be imposed on the legal entity (either controller or processor) that continues processing for direct marketing purposes when the data subject has objected to such processing. If the controller and/or the processor is an entrepreneur, the fine would be RSD 50,000, while the responsible person in the legal entity would be fined RSD 20,000.

11 Cookies

11.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

There are no special rules governing the application of cookies, beacons, the use of tracking technologies or behavioural advertising in Serbia.

However, the PDPA sets out the general rules that apply to the handling of personal data, including when processed in relation to cookies or similar tracking technologies. The most likely lawful basis for placing cookies or similar tracking technologies would be consent. It is obtained via an interactive website cookie banner that provides full disclosure of the different types of cookies and how the website user can accept or decline. Also, acceptance or rejection is not final, and the user can later change the settings related to cookies in the privacy policy. Notices that are not clearly visible due to colour refraction or font obscurity cannot be considered readily accessible.

In practice, when accessing the site for the first time, websites in Serbia typically do provide privacy information in relation to the use of cookies and similar tracking technologies via an interactive website cookie banner that provides full disclosure of the different types of cookies and how the website user can accept or decline. In most cases, websites do not display this kind of notification later, but only during the first access to the site and usually later, the user can change his or her decision by changing the settings related to cookies in the privacy policy.

11.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

No, as mentioned above, Serbia does not have a special legislation regarding the use of cookies and other tracking technologies.

11.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

We are not aware of any such activity of the Commissioner.

11.4 What are the maximum penalties for breaches of applicable cookie restrictions?

This is not applicable.

12 Restrictions on International Data Transfers

12.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Under the PDPA, international transfers of data to a country, territory or one or more specified sectors within that country, or an international organisation that ensures an adequate level of protection, do not require any prior authorisation (Articles 63 and 64 of the PDPA).

It is assumed that an adequate level of protection exists in:

- countries and international organisations that are parties to the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108);
- countries and international organisations that are considered by the EU to ensure adequate levels of protection of personal data; and
- countries with which the Republic of Serbia has concluded international treaties regarding the transfer of personal data (Article 64 of the PDPA).

The Serbian government has rendered the decision on the list of countries, parts of their territory or one or more specified sectors within those countries or international organisations that are considered to ensure the adequate level of personal data protection, which specifies the countries to which transfer of data is free.

Furthermore, under the PDPA, the transfer of personal data is also allowed to a country, a territory of, or one or more specified sectors within that country, or an international organisation that does not have an adequate level of protection if the controller or processor provides appropriate safeguards, and if enforceable data subject rights and effective legal remedies for data subjects are available in that country, a territory of, or one or more specified sectors within that country, or the relevant international organisation (Article 65 of the PDPA).

The appropriate safeguards may be provided by a controller without requiring any specific authorisation from the Commissioner by:

- a legally binding instrument between public authorities or bodies;
- standard data protection clauses prepared by the Commissioner that regulate the legal relationship between the controller and processor;
- binding corporate rules that regulate processing of personal data by a controller and the group of companies to which the controller belongs;
- an approved code of conduct, together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
- an approved certificate issued in accordance with the PDPA, together with binding and enforceable commitments on the part of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

The appropriate safeguards may also be provided through contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation, or through provisions inserted into administrative arrangements between public authorities or bodies that include enforceable

and effective data subject rights, but only with the specific authorisation of the Commissioner, which is obliged to give such an authorisation within 60 days from the day of receipt of the request for authorisation (Article 65 of the PDPA).

Further, under the PDPA, the data controller may introduce binding corporate rules that are adhered to by a controller or processor established in the territory of the Republic of Serbia for the purpose of a transfer, or a set of transfers, of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity. If the Commissioner approves the binding corporate rules, it is considered that a controller has provided adequate safeguards and that data may be transferred outside of the territory of the Republic of Serbia (Article 67 of the PDPA).

Nonetheless, each international transfer of data must be lawful, i.e. it must be based on one of the following legal grounds prescribed by the law:

- the data subject has given consent to the processing of their personal data for one or more specific purposes;
- it is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- it is necessary for compliance with a legal obligation to which the controller is subject;
- it is necessary in order to protect the vital interests of the data subject or of another natural person;
- it is necessary for the performance of a task carried out in the public interest or in the exercise of the official authority vested in the controller; or
- it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where those interests are overridden by those interests or fundamental rights and freedoms of the data subject that require the protection of personal data, in particular where the data subject is a child.

12.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

Businesses typically rely on standard contractual clauses for controller–processor relationships, which are prescribed by the Commissioner. Also, consent and performance of a contract with the data subject are also frequently used.

12.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

Under the PDPA, prior approval of the Commissioner may be required if data is to be transferred to a country that does not ensure an adequate level of protection (Article 65 of the PDPA). See above under question 12.1.

12.4 Do transfers of personal data to other jurisdictions require a transfer impact assessment? If conducting a transfer impact assessment is only mandatory in some circumstances, please identify those circumstances.

A transfer impact assessment is not mandatory under the PDPA.

12.5 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?

The Commissioner recommended the Serbian government to remove the USA from the list of countries, parts of their territory or one or more specified sectors within those countries or international organisations that are considered to ensure the adequate level of personal data protection, which specifies the countries to which transfer of data is free.

12.6 What guidance (if any) has/have the data protection authority(ies) issued in relation to the use of standard contractual/model clauses as a mechanism for international data transfers?

The Commissioner stipulated that these clauses must not be amended and may be used either as a separate agreement or part of an agreement that regulates other questions apart from the processing of personal data.

13 Whistle-blower Hotlines

13.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

Under the Whistleblower Protection Act, a whistle-blower is a natural person who performs whistleblowing with respect to his or her work engagement, employment procedure, use of services rendered by public and other authorities, holders of public powers or public services, business cooperation and right of ownership in a company. Any type of information can be disclosed (information regarding violation of regulations, violation of human rights, violation of public powers contrary to the purpose for which they were entrusted, danger to life, public health, safety and environment, as well as for the purpose of preventing damage of greater scope) and it may concern any person.

13.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous reporting is not prohibited under the Serbian Whistleblower Protection Act. Moreover, the law explicitly provides that employers are obliged not to undertake measures for discovering the identity of the anonymous whistle-blower. In practice, the employers conduct investigations on the basis of the provided information even in cases of anonymous reporting.

14 CCTV

14.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

The Serbian Law on Private Security provides that video surveillance must be indicated in a visible place when the object is under video surveillance. Also, video surveillance must not threaten the privacy of other people. Footage obtained through security cameras must be properly stored and must not be misused. The owner of the video surveillance is obliged to provide the footage only to the police upon request.

The PDPA does not contain specific provisions regulating the issue of monitoring premises with CCTV.

However, in the Commissioner’s Opinions on data processing at work, the Commissioner stated that in cases of video monitoring, the issue of the existence of a legal basis for such conduct must be taken into account for processing, the expediency and proportionality of processing in relation to the goal that is to be achieved by recording and the like. The above questions concern all personal data processing, including video surveillance which, in order to be considered permissible, must be in accordance with the provisions of the PDPA.

In this regard, it should be noted that video surveillance represents processing of personal data not only in those situations when it is carried out/makes a record of the monitoring of a natural person, i.e. when recording occurs systematically in a certain area, in a certain period of time, with the expectation of further review and/or use, but also in situations where no record is stored, i.e. when video surveillance represents only an “extended eye” of the employer.

The Commissioner also stated that it is not disputed that video surveillance can be introduced for the protection of company property and people’s safety. However, there is absolutely no justification for video surveillance to be carried out in offices, for example, in which employees perform administrative jobs. In principle, except in situations where working process due to high risks (for security, human health, national security, etc.) implies the existence of video surveillance, such as protection of personal data in the field of labour relations in a weapons factory, nuclear plant, certain laboratories, etc., such processing of personal data would be excessive, i.e. unnecessary, with a purpose that would be difficult to justify. It is especially unjustifiable to perform video surveillance in order to control the execution of work tasks on persons whose profession is such that it does not include one of the aforementioned risks.

Our view is that the permissibility of video monitoring should be evaluated in each individual case and based on all the details. However, our position is that, for example, the endangerment of certain goods/valuables and property would be considered as a valid legitimate interest for video surveillance installation and that would justify personal data processing. It can be concluded that it is acceptable to film corridors, empty rooms, entrances to offices or similar, where people pass by, but do not stay. However, an employer must not continuously film offices where people work and spend most of their working hours. There must be an important reason for the specific recording of work premises.

Also, it is hard to imagine that it would be justified to use CCTV in places where the employee has a reasonable expectation of privacy, e.g. toilets or changing rooms. In addition,

use of video surveillance inside lifts is prohibited as this is contrary to the principle of “data minimisation” unless there is an objective reason for such installation/use.

14.2 Are there limits on the purposes for which CCTV data may be used?

Under the Serbian Law on Private Security, CCTV data must be used only for the purpose for which it was collected and processed, and must not threaten or violate the privacy of other people. Footage obtained through security cameras must be properly stored and must not be misused. The owner of the video surveillance is obliged to provide the footage only to the police, upon request.

15 Employee Monitoring

15.1 What types of employee monitoring are permitted (if any), and in what circumstances?

In practice, pre-employment verifications are conducted on the basis of explicit consent. Monitoring during the employment (attendance, email, location of vehicles, monitoring premises with CCTV, call recording with customer services and alike) is most likely based on the employer’s legitimate interests, e.g. to ensure compliance with company policies and on the fulfilment of legal obligations. Legitimate interest requires a documented assessment of the employer’s (or a third party’s) legitimate interests (with a clearly defined purpose) that balances the aims of the monitoring against the likely impact on employees – if the interests of the employees outweigh the employer’s legitimate interests (for example, if the proposed monitoring is too intrusive), it is unlikely to be an appropriate lawful basis.

15.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

The Employment Act authorises the employer to monitor the work of its employees. The Workplace Safety and Health Act also obliges the employers to provide a safe and secure workplace for their employees. However, monitoring should not be too intrusive for the employees’ privacy. Therefore, in practice, employers frequently rely on legitimate interest in addition to law as a legal basis for monitoring, as well as on the employees’ consent. In any case, the employees must be informed about the monitoring.

15.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

There is no legal obligation to notify or consult works councils, trade unions or employee representatives regarding employee monitoring.

15.4 Are employers entitled to process information on an employee’s attendance in office (e.g., to monitor compliance with any internal return-to-office policies)?

Yes, on the basis of the provisions of the Serbian Employment Act.

16 Data Security and Data Breach

16.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Yes, both data controller and data processor have the obligation to ensure the security of personal data.

16.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Under the PDPA, a controller must notify a personal data breach to the Commissioner unless the breach is unlikely to result in a risk to interests of individuals.

Immediately upon becoming aware of a personal data breach, a controller must assess the likelihood and severity of the risk to individuals that could result from the breach.

If the breach is likely to result in a risk to the rights and freedoms of natural persons, the controller must without undue delay and not later than 72 hours after having become aware of the breach, notify the personal data breach to the Commissioner. Any delay in notification must be justified to the Commissioner.

The notification must at least:

- 1) describe the nature of the personal data breach, including where possible the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- 2) communicate the name and contact details of the DPO or other contact point where more information on the breach can be obtained;
- 3) describe the likely consequences of the personal data breach; and
- 4) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including measures taken to mitigate its possible adverse effects.

The Commissioner prescribed a form of this notification.

16.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Yes, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons. The controller must communicate the personal data breach to the data subject without undue delay and must describe in clear and plain language the incident, its impact, and measure taken to mitigate and heal the consequences of the incident.

The communication to the data subject shall not be required if:

- 1) the controller has implemented appropriate technical, organisational and personnel-related measures and those measures were applied to the personal data affected by the personal data breach, in particular encryption and

other measures that render the personal data unintelligible to any person who is not authorised to access it, including encryption;

- 2) the controller has taken subsequent measures that ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise; and
- 3) communication to the data subject would involve disproportionate use of time and resources – in such case, there shall be a public communication or similar measure by the controller whereby the data subjects are informed in an equally effective manner.

16.4 What are the maximum penalties for personal data security breaches?

A fine between RSD 50,000 and 2 million (i.e. max of EUR 17,000) will be issued to the controller or processor, who is a legal entity, for failure to notify the Commissioner or the individual whom the personal data breach concerns.

An entrepreneur will be fined between RSD 20,000 and 150,000 for failure to notify the Commissioner or the individual whom the personal data breach concerns.

The individual, who is the person responsible in a legal entity, a state authority, i.e. an authority of territorial autonomy and a local self-government unit, as well as a responsible person in a representative office or business unit of a foreign legal entity, will be fined between RSD 5,000 and 150,000 for failure to notify the Commissioner or the individual whom the personal data breach concerns.

Failure to notify a personal data breach to the Commissioner and/or individuals is not a criminal offence.

17 Enforcement and Sanctions

17.1 Describe the enforcement powers of the data protection authority(ies).

- (a) **Investigative powers:** Under the PDPA, the Commissioner has the power to:
 - order the controller and the processor, and, where applicable, their representatives, to provide all pieces of information that they require in exercising their powers;
 - check and assess the application of legal provisions and otherwise carry out supervision over protection of personal data by using his or her inspection powers;
 - verify compliance with the requirements for certification;
 - notify the controller and/or the processor of potential infringements of the PDPA;
 - request and obtain from the controller access to all pieces of personal data, as well as to information necessary for exercising their powers; and
 - request and obtain access to all the premises of the controllers and the processors, including access to all the means and equipment.
- (b) **Corrective powers:** Under the PDPA, in addition to the corrective powers identified above, the Commissioner has the power to:
 - issue warnings to a controller and to a processor through delivery of a written opinion that intended processing operations may infringe provisions of the PDPA;

- issue reprimands to a controller and/or to a processor where processing operations have infringed provisions of the PDPA;
 - order the controller and the processor to comply with the data subject's requests to exercise his or her rights, in compliance with the PDPA;
 - order the controller and the processor to bring processing operations into compliance with the provisions of the PDPA, in a precisely specified manner and within a precisely specified time limit;
 - order the controller to inform the data subject of a personal data breach;
 - impose a temporary or definitive limitation of performance of a processing;
 - order rectification and/or erasure of personal data or to limit performance of processing operations, as well as to order the controller to notify another controller, the data subject and the recipients to which the personal data has been disclosed or transmitted thereof;
 - withdraw a certificate or to order the certification body to withdraw a certificate issued pursuant to the PDPA, as well as to order the certification body to refuse to issue a certificate if the requirements for issuing thereof are not met;
 - impose a fine on the basis of a misdemeanour order, where it is determined in the course of an inspection supervision that a misdemeanour has been committed for which a fine of a fixed amount is prescribed by the PDPA, instead of other measures prescribed by this paragraph or in addition thereto, depending on the circumstances of each individual case; and
 - suspend transfer of personal data to a recipient in another country or to an international organisation.
- (c) **Authorisation and advisory powers:** The Commissioner advises legislative bodies on data protection measures, assists data subjects in exercising their rights, and collaborates with international supervisory authorities.
- (d) **Imposition of administrative fines for infringements of specified legal provisions:** Yes, the Commissioner is authorised to impose a fine that is determined in fixed amount for the following violations of the PDPA: (i) failure to acquaint the data recipient with specific conditions for processing provided by the law and its obligation of their fulfilment; (ii) failure to communicate to the data subject a justified decision; (iii) continuance of processing for direct marketing purposes when the data subject has objected to such processing; (iv) failure to appoint its representative in the Republic of Serbia; (v) failure to maintain prescribed processing records or to record processing activities; and (vi) failure to publish the contact details of the DPO and communicate them to the Commissioner. For other violations of the PDPA, the Commissioner is authorised to initiate misdemeanour proceedings before the competent courts who then impose a fine.
- (e) **Non-compliance with a data protection authority:** The Commissioner may initiate misdemeanour proceedings.

17.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

Yes, a court order is not required. However, the affected party

is authorised to challenge the Commissioner's order before the administrative court by filing a petition within 30 days as of the date of issuance of the order.

17.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

The Commissioner regularly exercise its powers.

17.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

The Commissioner sent a public invitation to large multi-national corporations such as Facebook, Google and alike for appointment of a representative in Serbia. However, we are not aware of the fact that the Commissioner imposed any fine toward the foreign legal entity. The reason for this could be the low amounts of fines prescribed by the PDPA compared to the costs and duration of the procedure for legal assistance between Serbia and other states.

18 E-discovery/Disclosure to Foreign Law Enforcement Agencies

18.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Businesses typically refuse to respond to foreign e-discovery requests, because under Serbian legislation, foreign law enforcement agencies should follow the procedure prescribed for international legal assistance in civil and criminal matters, which may be contained in the multilateral and/or bilateral interstates agreements, and contact the relevant state body, which would then request information from the Serbian entity.

18.2 What guidance has/have the data protection authority(ies) issued on disclosure of personal data to foreign law enforcement or governmental bodies?

We are not aware of any such guidelines.

19 Artificial Intelligence

19.1 Are there any limitations on automated decision-making involving the processing of personal data using artificial intelligence?

Artificial intelligence (AI) is still not regulated in Serbian legislation. Thus, general rules of the PDPA apply to automated decision-making involving the processing of personal data using AI.

19.2 What guidance (if any) has/have the data protection authority(ies) issued in relation to the processing of personal data in connection with artificial intelligence?

The Commissioner has not issued any guidelines with respect to AI.

20 Trends and Developments

20.1 In your opinion, what enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.

In December 2024, Amnesty International published a report, “A Digital Prison: Surveillance and the Suppression of Civil Society in Serbia”, stating that the Serbian authorities were using advanced surveillance technologies against political activists, journalists and members of the civil society. Political and environmental activists, journalists and members of the civil society who experienced unlawful surveillance were seriously concerned about their safety and confidentiality of their communications. Human rights organisations and civil society groups defined this practice as a serious violation of privacy, freedom of expression and freedom of assembly and requested the authorities to conduct serious investigations and punish those involved in this practice. State authorities did not comment further on this topic.

20.2 In your opinion, what “hot topics” are currently a focus for the data protection regulator?

In August 2023, the Government of the Republic of Serbia adopted the Personal Data Protection Strategy for the period of 2023 to 2030. One of the main goals of the Strategy is the improvement of the legislative framework in order to align it with the development and application of information and communication technologies in digitisation processes. In mid-January 2025, the working group responsible for preparing a draft of amendments of the PDPA held its first meeting. They announced that their work is to be focused on the introduction of legislation that is omitted from the current law but urgently needed such as legal regulation of cookies, video surveillance, AI and alike.



Vladimir Djerić advises and represents clients in matters concerning company, commercial and arbitration law, advertisement law, public international law and human rights. Vladimir Djerić has acted as counsel in international arbitrations (ICSID, ICC, UNCITRAL, Foreign Trade Court of Arbitration of the Serbian Chamber of Commerce) and before international courts and tribunals (ICJ, ECHR, ICTY). He has also served as an arbitrator (Arbitration of the Chamber of Commerce of Serbia, Foreign Trade Court of the Montenegrin Chamber of Commerce).

Mikijelj Jankovic & Bogdanovic
Vlajkovicева 28
Belgrade
Serbia

Tel: +381 11 3231 970
Email: vladimir.djeric@mjb.rs
LinkedIn: www.linkedin.com/in/vladimir-djeric-21b35647



Lena Petrovic focuses on litigation, data protection, advertising and media law. She represents clients in commercial and contract disputes as well as in disputes involving trademark and copyright infringements. She has also been involved in international arbitral proceedings.

Mikijelj Jankovic & Bogdanovic
Vlajkovicева 28
Belgrade
Serbia

Tel: +381 11 3231 970
Email: lena.petrovic@mjb.rs
URL: www.mjb.rs/en/our-team/lena-m-petrovic



Katarina Radovic provides advice on all aspects of labour law. She also advises clients on copyright law, and in particular specialises in copyright infringement litigation. Katarina Radovic provides assistance to our corporate clients on all aspects of their commercial transactions and has extensive experience in commercial law litigation before Serbian courts. Katarina Radovic is also a certified mediator.

Mikijelj Jankovic & Bogdanovic
Vlajkovicева 28
Belgrade
Serbia

Tel: +381 11 3231 970
Email: katarina.radovic@mjb.rs
LinkedIn: www.linkedin.com/in/katarina-radovic-04bbab275



Kristina Petronijevic joined Mikijelj Jankovic & Bogdanovic in 2023 as a graduate from Belgrade University, Faculty of Law. She assists senior members of our data protection and dispute resolution team in all aspects of their work.

Mikijelj Jankovic & Bogdanovic
Vlajkovicева 28
Belgrade
Serbia

Tel: +381 11 3231 970
Email: kristina.petronijevic@mjb.rs
LinkedIn: www.linkedin.com/in/kristina-petronijevic-330345298

Mikijelj Jankovic & Bogdanovic is a law firm established in 1985 in Belgrade, Serbia. We represent clients in over 30 countries with a particular focus on Serbia, Slovenia, Croatia, Bosnia and Herzegovina, Montenegro, Macedonia, Albania and Kosovo. Our law firm has been continuously recognised as a leader in the field of IP law and dispute resolution, and our attorneys are highly respected practitioners ranked by both *The Legal 500* (<https://www.legal500.com/c/serbia/intellectual-property>) and *Chambers and Partners* (<https://chambers.com/law-firm/mikijelj-jankovic-bogdanovic-europe-7:133442>). We have an extensive portfolio of clients that includes major international and domestic companies from the energy sector, food industry, pharmaceuticals, cosmetics, chemical industry, automotive industry, fashion, media and entertainment. A detailed list of our clients from a specific sector can be provided upon request. We also represent sovereign clients, as well as non-profit organisations, in matters of public and private law.

Since the early 1990s, Mikijelj Jankovic & Bogdanovic have also served as attorneys of confidence for a number of foreign embassies in Belgrade. We are proud that our sovereign clients include the embassies of Belgium, Canada, Denmark, Germany, Japan, Netherlands, Norway, Spain and Sweden. We take a personalised approach towards our clients, regardless of their size, and seek to provide them with the highest quality service.

www.mjb.rs



Singapore



Lim Chong Kin



Anastasia Su-Anne Chen

Drew & Napier LLC

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The Personal Data Protection Act 2012 (“**PDPA**”) is the principal data protection legislation in Singapore. The PDPA established a general data protection law which applies to all private-sector organisations.

In 2020, the PDPA underwent its first comprehensive review since its enactment. The amendments are set out in the Personal Data Protection (Amendment) Act 2020 (“**Amendment Act**”). The Amendment Act, which was passed in Parliament on 2 November 2020, sets out extensive amendments, which mostly came into effect on 1 February 2021.

Parts 3 to 6A of the PDPA set out obligations of organisations in respect of the collection, use, disclosure, access, correction, care, protection, retention, transfer of personal data and notification of data breaches (collectively, “**Data Protection Provisions**”); while Part 9 of the PDPA sets out provisions pertaining to Singapore’s national Do Not Call (“**DNC**”) Registry and the obligations of organisations in relation to sending marketing messages to Singapore telephone numbers (“**DNC Provisions**”).

Other regulations issued under the PDPA are:

- the Personal Data Protection Regulations 2021 (“**PDP Regulations**”), which set out the requirements for transfers of personal data out of Singapore; the form, manner and procedures for requests for access to or correction of personal data; and persons who may exercise rights in relation to disclosure of personal data of deceased individuals;
- the Personal Data Protection (Notification of Data Breaches) Regulations 2021 (“**Breach Notification Regulations**”);
- the Personal Data Protection (Composition of Offences) Regulations 2021;
- the Personal Data Protection (Do Not Call Registry) Regulations 2013;
- the Personal Data Protection (Enforcement) Regulations 2021; and
- the Personal Data Protection (Appeal) Regulations 2021.

In addition, the Personal Data Protection Commission (“**PDPC**”) has issued a number of advisory guidelines which provide greater clarity on the interpretation of the PDPA.

1.2 Is there any other general legislation that impacts data protection?

The Computer Misuse Act 1993 sets out a number of offences which include the unauthorised access or modification of computer material, as well as the unauthorised use or interception of computer services.

The Cybersecurity Act 2018 requires owners and operators of Critical Information Infrastructure to comply with cybersecurity policies and standards, conduct audits and risk assessments, and implement incident reporting measures.

For completeness, the Spam Control Act 2007 (“**SCA**”) regulates the bulk sending of unsolicited commercial electronic messages to email addresses or mobile telephone numbers, complementing the DNC Provisions of the PDPA.

1.3 Is there any sector-specific legislation that impacts data protection?

Yes, a number of other regulations and pieces of legislation in Singapore contain certain sector-specific data protection requirements. For example:

- the Banking Act 1970 (“**Banking Act**”) contains a number of banking secrecy provisions which govern customer information obtained by banks;
- the Telecom and Media Competition Code 2022 issued under the Telecommunications Act 1999 contains provisions governing the use of end-user service information by telecoms licensees; and
- the Healthcare Services Act 2020 (No. 3 of 2020), which replaces the Private Hospitals and Medical Clinics Act (Cap 248), contains provisions relating to the confidentiality of information held by healthcare service providers licensed under the Act.

With regard to the financial sector, the Monetary Authority of Singapore (“**MAS**”) is empowered under the Monetary Authority of Singapore Act 1970 and other sectoral legislation to issue directives and notices. Examples of MAS-issued regulatory instruments which are relevant to data protection include the Notices on Cyber Hygiene, Notices and Guidelines on Technology Risk Management, and the Guidelines on Outsourcing.

In this regard, Section 4(6) of the PDPA provides that the general data protection framework does not affect any right or obligation under other written laws, and that in the event of any inconsistency, the provisions of other written laws will prevail.

The PDPC has also developed sector-specific advisory guidelines for the telecommunications sector, the real estate agency sector, the education sector, the healthcare sector, the social services sector and transport services for hire (specifically in relation to in-vehicle recordings).

In addition, the PDPC has provided comments and suggestions to industry-led guidelines on the PDPA that were developed by industry associations such as:

- the Life Insurance Association Singapore (“LIA”) Code of Practice for Life Insurers on the Singapore Personal Data Protection Act; and
- the LIA Code of Conduct for Tied Agents of Life Insurers on the Singapore Personal Data Protection Act.

1.4 What authority(ies) are responsible for data protection?

The PDPC is responsible for administering and enforcing the PDPA. The PDPC is under the purview of the Ministry of Communications and Information (“MCI”), and is part of the merged info-communications and media regulator, the Info-communications Media Development Authority of Singapore (“IMDA”) (previously the Info-communications Development Authority of Singapore and the Media Development Authority of Singapore).

Sector-specific data protection obligations are separately enforced by the relevant sectoral regulators. For example, the MAS enforces the banking secrecy provisions under the Banking Act and other sectoral legislation and regulatory instruments governing other types of financial institutions.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **“Personal Data”**
“Personal data” is defined under the PDPA as data, whether true or not, about an individual who can be identified: (a) from that data; or (b) from that data and other information to which the organisation is likely to have access.
All formats of personal data are covered under the PDPA, whether electronic or non-electronic, and regardless of the degree of sensitivity.
- **“Processing”**
Under the PDPA, “processing”, in relation to personal data, means the carrying out of any operation or set of operations in relation to the personal data, and includes any of the following:
 - (a) recording;
 - (b) holding;
 - (c) organisation, adaptation or alteration;
 - (d) retrieval;
 - (e) combination;
 - (f) transmission; and
 - (g) erasure or destruction.
- **“Controller”**
The PDPA does not use the term “controller”, but instead refers to an “organisation”. An “organisation” is defined as any individual, company, association or body of persons, corporate or unincorporated, whether or not:
 - (a) formed or recognised under the law of Singapore; or
 - (b) resident, or having an office or a place of business, in Singapore.

- **“Processor”**
Similarly, the PDPA does not use the term “processor”, but instead refers to a “data intermediary”, which is defined as an organisation which processes personal data on behalf of another organisation but does not include an employee of that other organisation.
The PDPA provides that a data intermediary that processes personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing will only be subject to (i) the Protection Obligation, (ii) the Retention Limitation Obligation (as defined below), and (iii) the requirement to notify the data controller without undue delay where the data intermediary has reason to believe that a data breach has occurred in relation to personal data that it is processing on the data controller’s behalf.
- **“Data Subject”**
The PDPA does not use the term “data subject”, but instead refers generally to an “individual”, whose personal data is collected, used, disclosed, or otherwise processed by organisations. An “individual” is defined to mean a natural person, whether living or deceased.
- **“Sensitive Personal Data”/“Special Categories of Personal Data”**
The PDPA does not expressly distinguish between specific categories of personal data. The term “sensitive personal data” is not defined.
However, as a number of the Data Protection Provisions adopt a standard of reasonableness, the sensitivity of the personal data in question could, in practice, affect the application of the data protection obligations. For example, the PDPC has taken the position in several enforcement decisions that a higher standard of protection is required for more sensitive personal data, which includes insurance, medical and financial data (see *In Re Aviva Ltd* [2017] SGPDP 14).
In this regard, the PDPC’s Advisory Guidelines on Enforcement for Data Protection Provisions (“**Enforcement Guidelines**”) provide that, if an organisation which has breached a Data Protection Provision is in the business of handling large volumes of sensitive personal data, the disclosure of which may cause exceptional damage, injury or hardship to a person (such as medical or financial data), but failed to put in place adequate safeguards proportional to the harm that might be caused by disclosure of such personal data, the PDPC may also consider this to be an aggravating factor in calculating the level of the financial penalty to be imposed on the organisation.
Additionally, in the Breach Notification Regulations, the PDPC prescribes a list of personal data that, if subject to a data breach, would be deemed to result in significant harm to individuals. These include the following broad categories of personal data:
 - (a) financial information which is not publicly disclosed;
 - (b) personal data which would lead to the identification of vulnerable individuals (e.g. leading to identification of a minor who has been arrested for an offence);
 - (c) life, accident and health insurance information which is not publicly disclosed;
 - (d) specified medical information, including the assessment and diagnosis of HIV infections;
 - (e) information related to adoption matters;
 - (f) a private key used to authenticate any or digitally sign an electronic record or transaction; and

(g) an individual's account identifier and data for access into the individual's account.

■ “Data Breach”

“Data breach” is defined in Section 24 of the PDPA to mean: (a) the unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data; or (b) the loss of any storage medium or device on which personal data is stored in circumstances where the unauthorised access, collection, use, disclosure, copying, modification or disposal of the personal data is likely to occur.

■ “Business Contact Information”

“Business contact information” is defined in Section 2(1) of the PDPA to mean: an individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his or her personal purposes.

The Data Protection Provisions do not apply to “business contact information”.

3 Territorial and Material Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The PDPA applies to all organisations that are not a public agency, whether or not formed or recognised under the laws of Singapore, or resident or having an office or a place of business in Singapore.

According to the PDPC's Advisory Guidelines on Key Concepts in the PDPA (“**Key Concepts Guidelines**”), the Data Protection Provisions apply to organisations carrying out activities involving personal data in Singapore. Thus, where personal data is collected overseas and subsequently transferred into Singapore, the Data Protection Provisions will apply in respect of the activities involving the personal data in Singapore.

3.2 Do the data protection laws in your jurisdiction carve out certain processing activities from their material scope?

Yes. The Data Protection Provisions of the PDPA do not apply to individuals acting in a personal or domestic capacity. The PDPA also does not impose the Data Protection Provisions on an employee acting in the course of his employment within an organisation (Section 4(1)(a), (b) of the PDPA).

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

■ Transparency

Section 20 of the PDPA provides that an organisation must notify an individual of the purpose(s) for which it intends to collect, use or disclose his personal data, on or before such collection, use, or disclosure (“**Notification Obligation**”).

More generally, Sections 11 and 12 of the PDPA require an organisation to develop and implement policies and practices that are necessary for the organisation to meet its obligations under the PDPA, communicate such policies and practices to its employees, and make information about its policies and procedures publicly available (“**Accountability Obligation**”). Accountability under the PDPA requires organisations to undertake measures in order to ensure that they meet their obligations under the PDPA and, importantly, demonstrate that they can do so when required. The Accountability Obligation also requires an organisation to appoint a Data Protection Officer (“**DPO**”) (see section 8 below).

■ Lawful basis for processing

Sections 13 to 17 of the PDPA generally require that an organisation obtain the consent of an individual before collecting, using or disclosing his personal data for a purpose (“**Consent Obligation**”), unless an exception in the First or Second Schedule to the PDPA applies. Such consent from an individual must be validly obtained and may be either expressly given or deemed to have been given.

■ Purpose limitation

Section 18 of the PDPA provides that an organisation may collect, use or disclose personal data about an individual only for purposes that a reasonable person would consider appropriate in the circumstances and, where applicable, if the individual concerned has been notified (“**Purpose Limitation Obligation**”).

■ Data minimisation

The PDPA does not articulate the principle of data minimisation (i.e. the limitation of personal data collection to what is directly relevant and necessary to accomplish a specified purpose), although the Purpose Limitation Obligation and Retention Limitation Obligation (as defined below) operate to limit the collection, use, disclosure and retention of personal data by organisations to some extent.

Nonetheless, the PDPC recommends that organisations avoid the over-collection of personal data where this is not required for their business or legal purposes. Instead, the PDPC encourages organisations to consider whether there are alternative ways of addressing their requirements.

■ Proportionality

While the PDPA does not explicitly refer to the principle of proportionality, a number of the Data Protection Provisions – for instance, the Purpose Limitation Obligation, the Accuracy Obligation, the Protection Obligation and the Retention Limitation Obligation (as defined below) – refer to a standard of reasonableness.

More generally, Section 11(1) of the PDPA states that an organisation shall, in meeting its responsibilities under the PDPA, “consider what a reasonable person would consider appropriate in the circumstances”.

In this regard, the PDPC's Key Concepts Guidelines state that a “reasonable person” is judged based on an objective standard and can be said to be a person who exercises the appropriate care and judgment in the particular circumstances.

■ Retention

While the PDPA does not prescribe any specific data retention periods, Section 25 of the PDPA provides that an organisation must cease to retain documents containing personal data, or remove the means by which

the personal data can be associated with particular individuals as soon as it is reasonable to assume that (a) the purpose for which the personal data was collected is no longer being served by retention of the personal data, and (b) retention is no longer necessary for legal or business purposes (“**Retention Limitation Obligation**”).

■ **Accuracy**

Section 23 of the PDPA requires an organisation to make a reasonable effort to ensure that personal data collected by or on behalf of the organisation is accurate and complete, if the personal data is likely to be used by the organisation to make a decision that affects the individual to whom the personal data relates, or is likely to be disclosed by the organisation to another organisation (“**Accuracy Obligation**”).

■ **Protection**

Section 24 of the PDPA requires an organisation to make reasonable security arrangements to protect personal data in its possession or under its control, in order to prevent (i) unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks, and (ii) the loss of any storage medium or device on which personal data is stored. (“**Protection Obligation**”) (see our responses to section 16 below).

■ **Transfer Limitation**

Section 26 of the PDPA provides that an organisation must not transfer any personal data to a country or territory outside Singapore, except in accordance with prescribed requirements to ensure that the overseas recipient provides a standard of protection to the transferred personal data that is comparable to the protection under the PDPA (“**Transfer Limitation Obligation**”) (see our responses to section 12 below).

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

■ **Right of access to (copies of) data/information about processing**

Under Section 21 of the PDPA, an individual has the right to request an organisation to allow him access to his personal data.

Specifically, unless a relevant exception under the PDPA applies, an organisation is required to, on request by an individual, provide him with: (a) his personal data in the possession or under the control of the organisation; and (b) information about the ways in which that personal data has been or may have been used or disclosed by the organisation within a year before the date of the individual’s request (“**Access Obligation**”).

There are a number of exceptions to the Access Obligation. Specifically, an organisation is not required to provide an individual with his personal data or other information, in respect of the matters specified under the Fifth Schedule to the PDPA, which include, without limitation:

- opinion data kept solely for an evaluative purpose;
- personal data which, if disclosed, would reveal confidential commercial information that could, in the opinion of a reasonable person, harm the competitive position of the organisation;
- personal data collected, used or disclosed without consent, for the purposes of an investigation if

the investigation and associated proceedings and appeals have not been completed; and

- any request:
 - that would unreasonably interfere with the operations of the organisation because of the repetitious or systematic nature of the requests;
 - where the burden or expense of providing access would be unreasonable to the organisation or disproportionate to the individual’s interests;
 - for information that does not exist or cannot be found;
 - for information that is trivial; or
 - that is otherwise frivolous or vexatious.

In addition, Section 21(3) of the PDPA provides that an organisation shall not provide an individual with his personal data or other information, if doing so could be reasonably expected to:

- threaten the safety or physical or mental health of an individual other than the individual who made the request;
- cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request;
- reveal personal data about another individual;
- reveal the identity of an individual who has provided personal data about another individual and the individual providing the personal data does not consent to the disclosure of his identity; or
- be contrary to the national interest.

With respect to third-party personal data, certain exclusion(s) do not apply to any user activity data about, or any user-provided data from, the individual who made the request, despite such data containing personal data about another individual.

■ **Right to rectification of errors**

Under Section 22 of the PDPA, an individual has the right to request that an organisation correct an error or omission in his personal data.

Specifically, an organisation is required to, on request by an individual: (a) correct an error or omission in the individual’s personal data that is in the possession or under the control of the organisation; and (b) send the corrected personal data to every other organisation to which the personal data was disclosed by the organisation within a year before the date the correction request was made, unless that other organisation does not need the corrected personal data for any legal or business purpose (“**Correction Obligation**”).

However, Section 22(7) of the PDPA provides that an organisation is not required to comply with the Correction Obligation in respect of the following matters specified in the Sixth Schedule to the PDPA:

- opinion data kept solely for an evaluative purpose;
- any examination conducted by an education institution, examination scripts and, prior to the release of examination results, examination results;
- the personal data of the beneficiaries of a private trust kept solely for the purpose of administering the trust;
- personal data kept by an arbitral institution or a mediation centre solely for the purposes of arbitration or mediation proceedings administered by the arbitral institution or mediation centre;
- a document related to a prosecution if all proceedings related to the prosecution have not been completed; and
- derived personal data.

In addition, Section 22(6) of the PDPA provides that an organisation is not required to correct or otherwise alter an opinion, including a professional or an expert opinion.

- **Right to deletion/right to be forgotten**
The PDPA does not accord an individual the right to require an organisation to delete his personal data.
- **Right to object to processing**
Under Section 16 of the PDPA, an individual may, upon giving reasonable notice to an organisation, withdraw his consent (which includes deemed consent) given to the organisation for the collection, use or disclosure of his personal data for any purpose. Upon withdrawal of consent, the organisation must cease (and cause its data intermediaries and agents to cease) collecting, using or disclosing the personal data, as the case may be, unless the collection, use or disclosure of the personal data without consent is required or authorised under the PDPA or any other written law.
- **Right to restrict processing**
Please see our response to “Right to object to processing” above.
- **Right to data portability**
The Amendment Act has introduced a Data Portability Obligation, which is set out in Part 6B of the PDPA. However, it has yet to come into effect. Broadly, the Data Portability Obligation provides that subject to certain exceptions and conditions, upon an organisation’s receipt of a data porting request from an individual, the porting organisation must transmit the applicable data specified in the data porting request to the receiving organisation in accordance with any prescribed requirements.
- **Right to withdraw consent**
Please see our response to “Right to object to processing” above.
- **Right to object to marketing**
Please see our response to “Right to object to processing” above.
In addition, an individual who does not wish to receive specified telemarketing calls and messages addressed to his Singapore telephone number may register his Singapore telephone number on one or more of the three DNC registers (namely, the No Voice Call Register; the No Text Message Register; and the No Fax Message Register) (see our response to question 10.1 below).
- **Right protecting against solely automated decision-making and profiling**
The PDPA does not accord an individual a right against solely automated decision-making and profiling. However, individuals may withdraw consent, if they oppose to automated decision-making and profiling conducted by organisations. Please see our response to “Right to object to processing” above.
- **Right to complain to the relevant data protection authority(ies)**
An individual may lodge a complaint with the PDPC in respect of an organisation’s breach of any of the Data Protection Provisions or DNC Provisions. Upon receiving such a complaint, the PDPC may: direct the individual and the organisation to resolve the complaint; refer the matter for mediation; or conduct an investigation to determine whether or not the organisation is in compliance with the PDPA.

5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

The PDPA does not accord individuals the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

However, Section 48O of the PDPA confers upon individuals who have suffered loss or damage directly as a result of a contravention of the provisions of the PDPA the right to commence a private civil action.

6 Children’s Personal Data

6.1 What additional obligations apply to the processing of children’s personal data?

There are no specific provisions in the PDPA regulating the processing of children’s data.

Nevertheless, in its Advisory Guidelines on the PDPA for Selected Topics, the PDPC has stated that organisations should generally consider whether a minor has sufficient understanding of the nature and consequences of giving consent in determining whether the minor can effectively provide consent on his own behalf of the purposes of the PDPA.

The PDPC has also stated that as a practical rule of thumb, a minor who is at least 13 years of age would typically have sufficient understanding to be able to consent on his own behalf. However, it also states that where an organisation has reason to believe or it can be shown that a minor does not have sufficient understanding of the nature and consequences of giving consent, the organisation should obtain consent from an individual who is legally able to provide consent on the minor’s behalf, such as the minor’s parent or guardian.

On 28 March 2024, the PDPC published its Advisory Guidelines on the PDPA for Children’s Personal Data in the Digital Environment (“**Children’s Personal Data Guidelines**”). The Children’s Personal Data Guidelines apply to organisations whose online products or services are likely to be accessed by children.

The PDPC clarified that it considers that a child between 13 and 17 years old may give valid consent when the policies on the collection, use and disclosure of the child’s personal data, as well as the withdrawal of consent, are readily understandable to them. This includes ensuring that the child understands the consequences of providing and withdrawing his consent. If an organisation has reason to believe that a child does not have sufficient understanding of the nature and consequences of giving consent, the organisation should obtain consent from the parent or guardian.

The Children’s Personal Data Guidelines also state that the PDPC will consider the use of a child’s personal data or profile to target harmful or inappropriate content (as defined in the Code of Practice for Online Safety, issued under the Broadcasting Act 1994) as unreasonable. Additionally, children’s personal data are also to be generally considered as sensitive personal data and must be accorded a higher standard of protection under the PDPA.

Organisations are also advised to conduct data protection impact assessments before releasing products or services that are likely to be accessed by children in order to meet their Accountability Obligation under the PDPA.

7 Registration Formalities and Prior Approval

7.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

There is currently no requirement for organisations to register with or notify the PDPC.

7.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

This is not applicable in Singapore.

7.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

This is not applicable in Singapore.

7.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

This is not applicable in Singapore.

7.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

This is not applicable in Singapore.

7.6 What are the sanctions for failure to register/notify where required?

This is not applicable in Singapore.

7.7 What is the fee per registration/notification (if applicable)?

This is not applicable in Singapore.

7.8 How frequently must registrations/notifications be renewed (if applicable)?

This is not applicable in Singapore.

7.9 Is any prior approval required from the data protection regulator?

This is not applicable in Singapore.

7.10 Can the registration/notification be completed online?

This is not applicable in Singapore.

7.11 Is there a publicly available list of completed registrations/notifications?

This is not applicable in Singapore.

7.12 How long does a typical registration/notification process take?

This is not applicable in Singapore.

8 Appointment of a Data Protection Officer

8.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The appointment of a DPO is mandatory. Section 11(3) of the PDPA obliges an organisation to designate one or more individuals to be responsible for ensuring that the organisation complies with the PDPA.

The business contact information of at least one DPO must be made available to the public (e.g. email address or Singapore phone number) pursuant to Section 11(5) of the PDPA. This business contact information should be readily accessible from Singapore, operational during Singapore business hours and, in the case of telephone numbers, be Singapore telephone numbers. This is especially important if the DPO is not physically based in Singapore, as it would facilitate the organisation's ability to respond promptly to any complaint or query on its data protection policies and practices.

8.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

Generally, the PDPC may take the following enforcement actions against the organisation:

- (a) give the organisation such directions as the PDPC sees fit in the circumstances to ensure compliance; and/or
- (b) require the organisation to pay a financial penalty up to a maximum of 10% of the organisation's annual turnover in Singapore, or S\$1 million, whichever is higher.

8.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

The PDPA does not provide for any particular protections for DPOs in respect of their role as DPOs. However, to the extent that the DPO is an employee of the organisation, Section 4(1)(a) of the PDPA provides that the Data Protection Provisions do not apply to an employee acting in the course of his employment.

It should be noted that the appointment of a DPO does not relieve the organisation of its obligations and liabilities under the PDPA.

8.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

Yes. Section 11(3) of the PDPA only provides that each organisation “shall designate one or more individuals to be responsible for ensuring that the organisation complies with [the PDPA]”, but does not stipulate that organisations may not designate individuals already designated by other organisations. Section 11(4) of the PDPA further provides that an individual designated by an organisation may further delegate the responsibility to another individual. For the avoidance of doubt, the designated individual need not be an employee of the organisation.

8.5 Please describe any specific qualifications for the Data Protection Officer required by law.

There are no specific qualifications required by law of the DPO. In practice, however, it is advisable that an organisation appoint an individual (or a group of individuals) familiar with the data protection laws of Singapore, the organisation's data protection policies and procedures, as well as its data processing activities. This is to ensure that the DPO is well equipped to: (i) ensure the organisation's continued compliance with the PDPA; (ii) deal with any queries from authorities or the public in relation to the organisation's data protection practices; and (iii) limit the impact of any data breach incident.

The PDPC has also published the DPO Competency Framework and Training Roadmap to provide clarity on the competencies and proficiency levels that a DPO needs, and to assist organisations in the hiring and training of data protection professionals.

8.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

The DPO is responsible for ensuring the organisation's continued compliance with the PDPA. However, it should be noted that the appointment of a DPO does not relieve the organisation of its obligations and liabilities under the PDPA.

Some of the responsibilities of a DPO may include, but are not limited to:

- ensuring compliance with the PDPA, including developing and implementing policies and processes for handling personal data;
- fostering a data protection culture among employees and communicating personal data protection policies to stakeholders;
- managing personal data protection-related queries and complaints;
- alerting management to any risks that might arise with regard to personal data; and
- liaising with the PDPC on data protection matters, if necessary.

8.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

No, there is no requirement for the DPO to be registered with or notified to the PDPC. However, DPOs are encouraged to register themselves with the PDPC to gain access

to free workshops and resources, latest updates on the PDPA and best practices, exclusive networking events and insights on key trends for data breach prevention. DPOs may register themselves with the PDPC via its website, where they may keep abreast of developments in the PDPA and best practices: <https://www.pdpc.gov.sg/overview-of-pdpa/data-protection/business-owner/data-protection-officers>

8.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

No. However, under the PDPA, the business contact information of at least one DPO must be made available to the public. Under the PDP Regulations, this requirement is deemed to have been satisfied if the organisation makes available such information in any of the following manners:

- where the organisation is registered under an applicable Act – in a record relating to the organisation that is made available on the Internet website of the Accounting and Corporate Regulatory Authority at <https://www.bizfile.gov.sg> (at the time of writing, this website is unavailable); or
- in a readily accessible part of the organisation's official website.

9 Appointment of Processors

9.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

The PDPA does not expressly stipulate that an organisation must enter into an agreement with its data intermediary. However, it should be noted that appointing a data intermediary to process personal data does not relieve the organisation of its obligations and liabilities under the PDPA, as the organisation is deemed to “have the same obligation under [the PDPA] in respect of personal data processed on its behalf and for its purposes by a data intermediary as if the personal data were processed by the organisation itself”. In this regard, the PDPC's Guide to Managing Data Intermediaries states that the primary means by which an organisation may ensure appropriate protection of the personal data processed by its data intermediary is through a contract, and that it would be a breach of the PDPA if there is no contractual agreement or document setting out the key obligations and responsibilities of the data intermediary.

Further, the Advisory Guidelines on Key Concepts in the Personal Data Protection Act (“**Key Concepts Guidelines**”) state that it is important that an organisation is clear as to its rights and obligations when dealing with another organisation and, where appropriate, include provisions in their written contracts to clearly set out each organisation's responsibilities and liabilities in relation to the personal data in question, including whether one organisation is to process personal data on behalf of and for the purposes of the other organisation. Without clarity, the risks of any omissions will likely fall on the organisation, which as data controller, is ultimately responsible. If there is no contract evidenced or made in writing with the data organisation, the data intermediary may also be held directly responsible for the Data Protection Provisions in respect of the personal data that is processed on behalf of the data organisation.

9.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

As the organisation remains responsible for complying with the PDPA, notwithstanding that a data intermediary is processing personal data on its behalf, the organisation should set out clearly the responsibilities of all parties and impose specific obligations on its data intermediary through a written agreement, including restricting what the data intermediary may do with the disclosed personal data, having sufficient security measures to protect the disclosed personal data, and providing for audits, inspections or other types of spot checks to satisfy itself that the data intermediary is complying with the PDPA as well as exit management. The contractual terms should also reference a relevant international standard as the standard for protection of the personal data. In setting out the contract, the organisation should also consider and review details such as the schedules to the contract and other administrative instructions outside the contract. These can be developed in consultation with the data intermediary.

If it is contemplated that there will be overseas transfers of personal data, the agreement should provide assurances to ensure that the transferred personal data will remain protected to a standard comparable with the PDPA, along with other policies and practices (e.g. assurances of compliance with relevant industry standards/certification). See the “Transfer Limitation Obligation” at section 12 below.

10 Marketing

10.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

The PDPA and the SCA concurrently govern the sending of such direct marketing messages in Singapore.

Generally, where the personal data of an individual is collected, used and disclosed for marketing purposes, the consent of the individual concerned must be obtained and such consent must not have been obtained as a condition for the providing of a product or service where it would not be reasonably required to provide that product or service. This applies regardless of how the marketing communications are sent.

In this regard, the PDPC has noted in its Key Concepts Guidelines that a failure to opt out will not be regarded as consent in all situations, and has recommended that organisations obtain consent from an individual through a positive action of the individual. It would therefore be advisable to obtain prior opt-in consent instead.

In relation to the sending of marketing communications (i.e. “specified messages” as defined under Section 37 of the PDPA) by telephone call or text messaging (or fax) to a Singapore telephone number, the DNC Provisions of the PDPA require an organisation to:

- (a) obtain valid confirmation that the telephone number is not listed with the relevant DNC Register before sending the message or calling, unless clear and unambiguous consent to the sending of the specified message to that number is obtained in evidential form;
- (b) include information identifying the sender for messages and details on how the sender can be readily contacted

and such details and contact information should be reasonably likely to be valid for at least 30 days after the sending of the message;

- (c) for voice calls, not conceal or withhold the calling line identity from the recipient; and
- (d) not to send, cause to be sent, or authorise the sending of an applicable message to any telephone number generated or obtained through the use of: (i) a dictionary attack; or (ii) address-harvesting software.

In relation to the sending of unsolicited marketing communications in bulk by email, instant messaging or other electronic messaging means, Section 11 read with the Second Schedule of the SCA stipulates that such messages must contain, *inter alia*, the following:

- (a) information on the sender;
- (b) a clear and conspicuous statement in English setting out the procedure to unsubscribe;
- (c) a title in its subject field that is not false or misleading as to the content of the message;
- (d) a label “<ADV>” with a space before the title of the subject field or, in the absence of a subject field, the first word of the message;
- (e) header information that is not false or misleading; and
- (f) an accurate and functional email address or telephone number by which the sender is readily contactable.

The unsubscribe facility must be legitimately obtained, valid and capable of receiving the unsubscribe request and a reasonable number of similar unsubscribe requests sent by other recipients at all times within at least 30 days after the unsolicited message is sent. No further unsolicited marketing communications can be sent after 10 business days following the date of the unsubscribe request.

Furthermore, Section 9 of the SCA prohibits unsolicited commercial electronic messages in bulk from being sent to electronic addresses generated or obtained through the use of a dictionary attack or address-harvesting software.

10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

Generally, the direct marketing restrictions in the PDPA only apply in the business-to-consumer (“B2C”) context where an organisation sends direct marketing communications to individual consumers. Insofar as an organisation sends direct marketing messages to another organisation through the use of business contact information, i.e. business-to-business (“B2B”) messages, the PDPA would likely not be applicable in those instances.

Specifically in relation to the sending of specified messages (as defined in Section 37 of the PDPA) by telephone call, text messaging, or fax to a Singapore telephone number, paragraph 1(g) of the Eighth Schedule of the PDPA provides that a “specified message” shall exclude “any message sent to an organisation other than an individual acting in a personal or domestic capacity, for any purpose of the receiving organisation”. In other words, a B2B marketing message would not be considered a “specified message”, and the organisation that sent such a B2B message would not need to comply with requirements under the DNC Provisions.

Notwithstanding, B2B marketing is currently covered under the SCA, and the restrictions on such electronic messages (see question 10.1 above) would similarly apply.

10.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

Please see our response to question 10.1 above.

10.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Yes, insofar as an organisation collects, uses or discloses personal data in Singapore (e.g. collects the personal data from individuals in Singapore for marketing purposes), the Data Protection Provisions of the PDPA would apply to such organisation, whether or not the organisation is formed or recognised under the laws of Singapore, or resident or having an office or a place of business in Singapore.

Specifically, the DNC Provisions under the PDPA apply when the sender of the specified message is present in Singapore when the specified message is sent, or the recipient of the specified message is present in Singapore when the specified message is accessed.

The SCA applies as long as the electronic message has a Singapore link, which includes, *inter alia*, the following situations:

- the message originates in Singapore or the sender of the message is: (i) an individual who is physically present in Singapore when the message is sent; or (ii) an entity which is formed or recognised under the law of Singapore, or which has an office or a place of business in Singapore;
- the computer, mobile telephone, server or device that is used to access the message is located in Singapore; or
- the recipient of the message is, when the message is accessed: (i) an individual who is physically present in Singapore; or (ii) an entity that carries on business or activities in Singapore.

10.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

The PDPA is a complaints-based regime and the PDPC has been active in the enforcement of breaches thereof.

Since the commencement of the PDPA in 2014, the PDPC has charged several individuals for offences relating to breaches of the DNC Registry.

10.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Purchasing marketing lists from third parties is only lawful if the individuals whose personal data is contained within the lists are notified of, and consent to, the sale of their personal data before such data is collected, used and/or disclosed.

The purchase of marketing lists constitutes collecting personal data under the PDPA. The PDPC has taken enforcement action against organisations which have purchased marketing lists without obtaining valid consent. For example, in the decision of *Re Sharon Assya Qadriyah Tang* [2018] SGPDP 1, the PDPC imposed a financial penalty of S\$6,000 on an individual for buying and selling marketing lists containing personal data.

Similarly, the PDPC took action in the case of *Re Amicus Solutions Pte Ltd & Anor* [2019] SGPDP 33, which involved the unauthorised sale and disclosure of personal data by a data broker for telemarketing purposes. In that case, the PDPC stated that organisations that sell datasets should ensure that they obtain and maintain clear records of consent so that proper assurances can be given to buyers. Correspondingly, buyers should undertake proper due diligence, such as seeking written confirmation that the personal data sold was actually obtained via legal sources or means, or inquire further as to whether the individuals were notified of the disclosure and had provided consent, and if so, obtain a sample of such notification and consent. On the facts, the PDPC imposed a fine of S\$48,000 on the data seller (including the S\$2,900 for the profit that the seller made from the sale of the datasets), and a fine of S\$10,000 on the buyer.

10.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

In relation to a breach of the Data Protection Provisions that apply to the sending of marketing communications, the organisation may find itself liable to pay a financial penalty of up to S\$1 million or 10% of the organisation's annual turnover in Singapore, whichever is higher. See question 8.2 above.

In relation to the DNC Provisions, the Amendment Act brings contraventions of the DNC Provisions (which used to be enforced as criminal offences), under the same administrative regime as the Data Protection Provisions. Accordingly, if the organisation is found to have intentionally or negligently contravened any provision, the PDPC may require the organisation to pay a financial penalty not exceeding:

- (a) S\$200,000, in case of an individual; or
- (b) S\$1 million, in any other case.

For contravention of the provisions prohibiting the use of dictionary attacks and address-harvesting software under the DNC Provisions, the maximum financial penalty has been increased to 5% of the annual turnover of the organisation in Singapore, where the annual turnover in Singapore exceeds S\$20 million.

These offences are in addition to the rights of private action that individuals may have against the organisation under the PDPA and the SCA.

11 Cookies

11.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

There are presently no legislative restrictions on the use of cookies or similar technologies *per se*, although the PDPA will apply to cookies that collect or use personal data.

According to the Advisory Guidelines on the PDPA for Selected Topics, for Internet activities that the user has clearly requested (e.g. transmitting personal data for effecting online communications and storing information that the user enters in a web form to facilitate an online purchase), there may not be a need to seek consent for the use of cookies to collect, use and disclose personal data where the individual is aware of the purposes for such collection, use or disclosure and voluntarily provided his personal data for such purposes. For activities that cannot take place without cookies that collect, use or disclose personal data, consent may be deemed if the

individual voluntarily provides the personal data for that purpose of the activity, and it is reasonable that he would do so. The Guidelines also clarify that the mere failure of an individual to actively manage his browser settings does not imply that the individual has consented to the collection, use and disclosure of his personal data by all websites for their stated purpose.

11.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

This is not applicable in Singapore.

11.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

This is not applicable in Singapore.

11.4 What are the maximum penalties for breaches of applicable cookie restrictions?

This is not applicable in Singapore.

12 Restrictions on International Data Transfers

12.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

The Transfer Limitation Obligation under the PDPA requires organisations transferring personal data overseas to do so only in accordance with the requirements prescribed under the PDPA to ensure that the recipients provide the transferred personal data a standard of protection that is comparable to the PDPA.

In particular, under the PDP Regulations, the transferring organisation must, before transferring the personal data outside of Singapore, take appropriate steps to ascertain whether, and to ensure that, the recipient is bound by legally enforceable obligations to provide the transferred personal data with a standard of protection comparable to that under the PDPA.

Pursuant to Regulation 11(1) of the PDP Regulations, “legally enforceable obligations” include obligations imposed on the recipient under:

- (a) any law;
- (b) any contract that requires the recipient to provide to the transferred personal data a standard of protection that is at least comparable to the protection under the PDPA, and which specifies the countries and territories to which the personal data may be transferred under the contract;
- (c) any binding corporate rules (in cases where a recipient is an organisation related to the transferring organisation) that require every recipient to provide to the transferred personal data a standard of protection that is at least comparable to the protection under the PDPA, and which specifies (i) the recipients of the transferred personal data to which the binding corporate rules apply, (ii) the countries and territories to which the personal data may be transferred under the binding corporate rules, and

- (iii) the rights and obligations provided by the binding corporate rules; or
- (d) any other legally binding instrument.

In relation to binding corporate rules, the PDP Regulations define a recipient as being related to the transferring organisation if:

- (a) the recipient, directly or indirectly, controls the transferring organisation;
- (b) the recipient is, directly or indirectly, controlled by the transferring organisation; or
- (c) the recipient and the transferring organisation are, directly or indirectly, under the control of a common person.

For completeness, the PDP Regulations provide for certain prescribed situations whereby the Transfer Limitation Obligation is taken to be satisfied and it is not necessary to legally impose enforcement obligations, e.g. where the personal data is publicly available in Singapore or where the personal data is data in transit.

The PDP Regulations also recognise the certification systems under the Asia-Pacific Economic Cooperation (“APEC”) Cross-Border Privacy Rules (“CBPR”) System and Privacy Recognition for Processors (“PRP”) System as one of the modes for the transfers of data overseas. If the recipient holds a specified certification (i.e. certification under the APEC CBPR/PRP) that is granted or recognised under the law of that country or territory to which the personal data is transferred, the recipient is taken to be bound by legally enforceable obligations to provide a standard of protection for the transferred personal data that is at least comparable to the protection under the PDPA.

12.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

Companies generally rely on robust data transfer agreements and binding corporate rules, as well as active enforcement of the terms of these documents, to ensure their compliance with applicable transfer restrictions.

See also questions 9.1 and 9.2 above with respect to overseas transfers of personal data for organisations engaging data intermediaries.

12.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

No, there is no requirement for registration/notification or prior approval from the PDPC for transfers of personal data abroad.

12.4 Do transfers of personal data to other jurisdictions require a transfer impact assessment? If conducting a transfer impact assessment is only mandatory in some circumstances, please identify those circumstances.

The PDPA does not require organisations to carry out a

transfer impact assessment (which is not a term defined under the PDPA) when transferring personal data outside of Singapore. There is no express requirement to assess whether the laws and practices in the third country prevent the overseas recipient from providing the requisite standard of protection, in particular, taking into account the rights of access and surveillance by the third country's public authorities.

However, for clarity, one of the available transfer mechanisms under the PDPA is for the transferring organisation to assess and determine that the foreign national laws governing the overseas recipient of the transferred personal data provides a standard of protection comparable to that under the PDPA (i.e. this is a way of ensuring that there are legally enforceable obligations imposed on the recipient, pursuant to Regulation 11(1)(a) of the PDP Regulations).

12.5 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?

The PDPC has not issued any guidance on this topic.

12.6 What guidance (if any) has/have the data protection authority(ies) issued in relation to the use of standard contractual/model clauses as a mechanism for international data transfers?

The PDPC, in collaboration with ASEAN and the EU, has published a Joint Guide to ASEAN Model Contractual Clauses ("ASEAN MCCs") and EU Standard Contractual Clauses ("EU SCCs"), which was updated on 31 January 2024. The non-binding guide, which comprises a Reference Guide and an Implementation Guide, provides organisations looking to transfer or receive data from overseas partners with a comparison between the ASEAN MCCs and EU SCCs and examples of best practices that can be implemented to operationalise safeguards required under the ASEAN MCCs and EU SCCs.

13 Whistle-blower Hotlines

13.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

The PDPA does not specifically regulate corporate whistle-blowing hotlines.

To the extent that whistle-blowing falls under the definition of "investigation" as found in the PDPA, the PDPA provides that personal data can be collected without obtaining consent if it is necessary for any investigation or proceedings. Similarly, the use and disclosure of personal data can be done without obtaining consent if it is necessary for any investigation or proceedings.

In this regard, the PDPA defines "investigation" to refer to an investigation relating to:

- (a) a breach of an agreement;
- (b) a contravention of any written law, or any rule of professional conduct or other requirement imposed by any regulatory authority in exercise of its powers under any written law; or

- (c) a circumstance or conduct that may result in a remedy or relief being available under any law.

The PDPA also provides for a broad definition of "proceedings" to mean any civil, criminal or administrative proceedings by or before a court, tribunal or regulatory authority that is related to the allegation of:

- (a) a breach of an agreement;
- (b) a contravention of any written law or any rule of professional conduct or other requirement imposed by any regulatory authority in exercise of its powers under any written law; or
- (c) a wrong or a breach of a duty for which a remedy is claimed under any law.

13.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous reporting is not regulated under the PDPA.

14 CCTV

14.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

The PDPA does not require the use of CCTV to be separately registered/notified or approved beforehand by the PDPC. However, as video and audio recordings of individuals may constitute personal data, the use of CCTV may constitute the collection of personal data and hence an organisation must comply with the PDPA when using CCTV.

According to the PDPC's Advisory Guidelines on the PDPA for Selected Topics, the PDPC recommends that notices or other forms of notification should generally be placed at locations that would enable individuals to have sufficient awareness that CCTV has been deployed for a particular purpose. Generally, organisations should indicate that CCTV is operating in the premises, and state the purpose of the CCTV (e.g. the CCTV is installed for security purposes) if such purpose may not be obvious to the individual. Further, where the CCTV deployed records both video and audio, organisations should indicate that both video and audio recordings are taking place.

14.2 Are there limits on the purposes for which CCTV data may be used?

Insofar as CCTV data contains personal data, the PDPA limits the purposes for which the CCTV data may be used.

15 Employee Monitoring

15.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Employee monitoring is not specifically regulated in Singapore. To the extent that the employee monitoring results in the collection, use or disclosure of personal data under the PDPA, such monitoring must comply with the Data Protection Provisions.

15.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Employers are generally required to provide suitable notices and obtain consent, before collecting, using or disclosing the personal data of their employees.

However, the PDPA provides for an exception to consent where personal data is collected by the employer and the collection for the purpose of or in relation to the organisation: (a) entering into an employment relationship with the individual or appointing the individual to any office; or (b) managing or terminating the employment relationship with or appointment of the individual. Nonetheless, if the organisation wishes to rely on this exception, the organisation would need to inform the individual of the purpose, and on request by the individual, the contact information of a person who is able to answer the individual's questions on such processing.

The "legitimate interests" exception to consent may also be applicable. However, the organisation would similarly need to notify the individual that it is relying on the exception for such purposes (and comply with other conditions).

15.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

As the relationship between employers and trade unions is very much subject to the terms of the collective agreement, the necessity of notifying or consulting the trade union in respect of CCTV and employee monitoring is dependent on the terms of the collective agreement. There are generally no legal requirements under Singapore law requiring works councils/trade unions/employee representatives to be notified or consulted.

15.4 Are employers entitled to process information on an employee's attendance in office (e.g., to monitor compliance with any internal return-to-office policies)?

Employers can process information on an employee's attendance in office for reasons such as monitoring compliance with internal return-to-office policies without the employee's consent if this is reasonable for managing the employment relationship. However, the employers must first notify their employees of the purposes of processing of personal data. Please see our response to question 15.2 above for more information on this exception.

16 Data Security and Data Breach

16.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Yes, both organisations and data intermediaries are subject to the Protection Obligation in relation to the personal data in their possession or control. For the Protection Obligation, please see our response to question 4.1 above.

While the PDPC has recognised that there is no one-size-fits-all solution, it has, in its Key Concepts Guidelines, noted that an organisation should:

- design and organise its security arrangements to fit the nature of the personal data held by the organisation

and the possible harm that might result from a security breach;

- identify reliable and well-trained personnel responsible for ensuring information security;
- implement robust policies and procedures for ensuring appropriate levels of security for personal data of varying levels of sensitivity; and
- be prepared and able to respond to information security breaches promptly and effectively.

16.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

There is a mandatory data breach notification regime under Part 6A of the PDPA, which broadly requires organisations to notify the PDPC of a "notifiable data breach".

Duty to assess

Section 26C of the PDPA requires organisations to conduct, in a reasonable and expeditious manner, an assessment of whether the data breach is a notifiable data breach, if it has reason to believe that a data breach has occurred affecting personal data in its possession or under its control.

Where a data intermediary has reason to believe that a data breach has occurred in relation to personal data that the data intermediary is processing on behalf of and for the purposes of another organisation, the data intermediary must, without undue delay, notify that other organisation of the occurrence of the data breach.

Requirement to notify

Under Section 26D of the PDPA, a data breach is a "notifiable data breach" if it:

- results in, or is likely to result in, significant harm to the individuals to whom the data relates (including if the breach relates to prescribed types of data); or
- is, or is likely to be, of a significant scale (i.e. the data breach involves personal data of 500 or more individuals).

The organisation must notify the PDPC as soon as is practicable, but in any case, no later than three calendar days after it makes the assessment.

The notification should be in the form and manner as prescribed in the Personal Data Protection (Notification of Data Breaches) Regulations 2021 and contain information to the best of the knowledge and belief of the organisation at the time.

Details of notification

Specifically, the notification to the PDPC should include information such as:

- the date and circumstances in which the organisation first became aware that the data breach had occurred;
- an account of steps taken afterwards, including the organisation's assessment of whether the breach is notifiable;
- how the data breach occurred;
- the number of individuals affected by the data breach;
- the personal data or classes of personal data affected;
- the potential harm to the affected individuals as a result;

- any action by the organisation to: (i) eliminate or mitigate any potential harm to any affected individual; and (ii) address or remedy any failure or shortcoming that resulted in the breach;
- the organisation's plan to inform all or any affected individuals or the public or grounds for not informing the affected individuals (if applicable);
- the business contact information of at least one authorised representative; and
- the reasons for late notification and/or the grounds for not notifying affected individuals (if the organisation is otherwise required to notify), where applicable.

Notification to the PDPC is to be submitted at <https://eservice.pdpc.gov.sg/case/db>. For urgent notification of major cases, organisations may also contact the PDPC at +65 6377 3131 during working hours.

The PDPC's Guide on Managing and Notifying Data Breaches (updated 15 March 2021) provides further guidance to help organisations to identify, prepare for and manage data breaches.

In addition to the Data Breach Notification Obligation under the PDPA, there may also be sector-specific requirements relating to the notification of data breaches to which the organisation is subject.

16.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Under Section 26D of the PDPA, organisations must, on or after notifying the PDPC, notify the individuals affected by a notifiable data breach, if the data breach results in, or is likely to result in, significant harm to an affected individual, unless either one of the stated exceptions apply, namely:

- where the organisation has taken remedial action that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual;
- where the organisation has implemented any technological measure (e.g. encryption) that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual; or
- if the organisation is instructed by a prescribed law enforcement agency, or directed by the PDPC, not to notify any affected individual.

In addition, the PDPC may, on written application, waive the requirement in exceptional circumstances where notification to affected individuals may not be desirable.

The notification to affected individuals should contain the following:

- the circumstances in which the organisation first became aware that the data breach had occurred;
- the personal data or classes of personal data affected;
- the potential harm to the affected individuals as a result;
- any action by the organisation to: (i) eliminate or mitigate any potential harm to any affected individual; and (ii) address or remedy any failure or shortcoming that resulted in the breach;
- the steps that the affected individual may take to eliminate or mitigate any potential harm as a result, including preventing the misuse of the data; and
- contact details of at least one authorised representative whom the affected individual can contact for further information or assistance.

The notification should be in the form and manner as prescribed in the Personal Data Protection (Notification of Data Breaches) Regulations 2021 and contain information to the best of the knowledge and belief of the organisation at the time.

16.4 What are the maximum penalties for personal data security breaches?

The PDPC has discretion to issue such remedial directions as it sees fit, including a notice to require payment of a financial penalty of up to a maximum of 10% of the organisation's annual turnover in Singapore, or S\$1 million, whichever is higher.

On 15 January 2019, the PDPC imposed its highest financial penalties to date, of S\$250,000 and S\$750,000, respectively, on SingHealth Services Pte Ltd ("SingHealth") and Integrated Health Information Systems Pte Ltd, for breaching their data protection obligations under the PDPA. This unprecedented data breach, which arose from a cyberattack on SingHealth's patient database system, caused the personal data of some 1.5 million patients to be compromised.

17 Enforcement and Sanctions

17.1 Describe the enforcement powers of the data protection authority(ies).

- (a) **Investigative powers:** The Ninth Schedule of the PDPA sets out extensive powers of investigation of the PDPC and its inspectors, which includes the power to: (i) require documents or information; (ii) require provision of information (e.g. to require attendance of individuals); and (iii) enter premises with or without a court-issued search warrant.

Section 51 of the PDPA sets out certain offences relating to, amongst others, obstructing or hindering the PDPC in the performance of any function or duty, or the exercise of any power, under the PDPA. It is also an offence for an organisation or a person, without reasonable excuse, to neglect or refuse to either provide any information or produce any document which the organisation or person is required to provide or produce to the PDPC or an inspector, or attend before the PDPC or inspector as required.

- (b) **Corrective powers:** Under Section 48H of the PDPA, upon a complainant's application, the PDPC may review: (i) refusals to provide access to personal data or to correct personal data as requested by the complainant under the PDPA or a failure to provide such access or correction within a reasonable time; and (ii) a fee required from the complainant by an organisation in relation to a request by the complainant under the PDPA.

Upon reviewing, the PDPC may: (i) confirm the refusal to provide access to or correct the personal data (as the case may be) or direct the organisation to provide access to or correct the personal data (as the case may be) within a specified timeframe; or (ii) confirm, reduce or disallow a fee, or direct the organisation to make a refund to the complainant.

- (c) **Authorisation and advisory powers:**

- Voluntary undertakings

Section 48L of the PDPA empowers the PDPC to accept statutory undertakings. Under this new

Section, where the PDPC has reasonable grounds to believe that an organisation has not complied, is not complying or is likely not to comply with any of the Data Protection Provisions, the organisation may give, and the PDPC may accept a written voluntary undertaking.

■ **Alternative dispute resolution**

Section 48G of the PDPA empowers the PDPC to establish or approve one or more dispute resolution schemes for the resolution of complaints by mediation, and to make regulations relating to the operation of such schemes. The PDPC may, with or without the parties' consent, refer the matter to mediation under a dispute resolution scheme, if it is of the view that the matter may more appropriately be resolved in this manner.

The PDPC has issued a Guide on Active Enforcement which articulates the PDPC's approach in deploying its enforcement powers to act effectively and efficiently in the event of data breach incidents. The guide also reiterates the PDPC's general approach to maximise the use of facilitation and mediation in seeking a resolution between the complainant and the organisation concerned.

- (d) **Imposition of administrative fines for infringements of specified legal provisions:** In the context of Singapore, the PDPC may impose a financial penalty of up to a maximum of 10% of the organisation's annual turnover in Singapore, or S\$1 million, whichever is higher, for breaches of the Data Protection Provisions in the PDPA.

In the event of a breach of the DNC Provisions of the PDPA, the PDPC may require the organisation to pay a financial penalty not exceeding:

- (a) S\$200,000, in case of an individual; or
- (b) S\$1 million, in any other case,

except that for contravention of the provisions prohibiting the use of dictionary attacks and address-harvesting software under the DNC Provisions, the maximum financial penalty has been increased to 5% of the annual turnover of the organisation in Singapore, where the annual turnover in Singapore exceeds S\$20 million.

- (e) **Non-compliance with a data protection authority:** If the PDPC is satisfied that: (a) an organisation has not complied or is not complying with any provision of the Data Protection Provisions; or (b) a person has not complied or is not complying with any of the DNC Provisions, the PDPC may issue such directions as it thinks fit in the circumstances to ensure compliance by an organisation with the PDPA. These include, but are not limited to, directions to: (i) stop collecting, using or disclosing personal data in contravention of the PDPA; (ii) destroy personal data collected in contravention of the PDPA; (iii) comply with any direction of the PDPC; and (iv) pay a financial penalty. (Please see question 17.1(d) above on the quantum of the financial penalty.)

17.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The PDPC is empowered to direct an organisation to stop collecting, using or disclosing personal data in contravention of the PDPA.

The PDPC does not require a court order to issue directions. Nonetheless, the PDPC may apply for the direction to be registered in a District Court for the purposes of enforcement by the court.

17.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

The PDPC takes a pragmatic approach in administering and enforcing the PDPA and aims to balance the need to protect individuals' personal data and the needs of organisations to use the data for legitimate purposes.

Since 2016, the PDPC has published over 250 enforcement decisions, with a significant majority of these cases relating to breaches of the Protection Obligation. In respect of these cases, the PDPC has either issued the organisation a warning, or imposed directions requiring the infringing organisation to take remedial action and to pay financial penalties.

Examples of recent cases include the following:

- A financial penalty of S\$20,000 was imposed on the Consumers' Association of Singapore (a non-profit, non-governmental organisation which aims to protect consumer interests) for its breach of the Protection and Accountability Obligations in respect of two data breach incidents. The first incident involved a threat actor signing into the organisation's email accounts using login credentials that were likely obtained from a successful phishing attack on an employee. The threat actor was thereby able to harvest consumers' email addresses from the organisation's mailboxes and send phishing emails on behalf of the organisation with the organisation's verified domain name. Three individuals suffered monetary losses. The second incident relates to the sending of phishing emails to consumers (which contained the details of their original complaints to the organisation) but not from the organisation's domain. The exfiltration of such data likely arose when the organisation migrated data from one vendor to another. With regard to the Protection Obligation, the PDPC found that the organisation's password management policy was manifestly insufficient. It failed to enforce the minimum character-length stated in its Password Complexity Policy, and did not adopt/enforce how frequently passwords ought to be changed. The organisation also failed to stipulate clear security responsibilities in its vendor contracts and conduct staff training. With regard to the Accountability Obligation, the Organisation failed to have any ICT policies to cover critical aspects in its IT security, among other things. In determining the financial penalty, the Commission also considered the organisation's turnover.
- A financial penalty of S\$120,000 was imposed on Keppel Telecommunications & Transportation for a breach of the Protection Obligation under the PDPC. The PDPC found that the organisation had failed to implement reasonable security arrangements to protect the personal data of employees, ex-employees, directors and shareholders in its possession or under its control. Notably, the PDPC observed that the long period of the organisation's breach of the Protection Obligation (i.e. more than two years), and the organisation's failure to provide clear instructions and supervise staff during its data migration and divestment (in particular, to delete its personal data from the affected server belonging to

the divested entity) revealed systemic shortcomings in the organisation's data protection processes. The PDPC also noted that the affected data included specimen signatures, bank account numbers, full images of identification cards, among others, which exposed individuals to greater risks of identity theft or financial losses. In determining the financial penalty, the Commission also considered the organisation's turnover to ensure the penalty would be an effective deterrent.

- A financial penalty of S\$7,000 was imposed on Tok Leng Leng t/a Top Mobile Gallery (BR) for breaching the Protection Obligation under the PDPA. The organisation had failed to implement reasonable security arrangements to protect against the unauthorised use of and access to customers' personal data for registration of pre-paid SIM cards. Specifically, the organisation did not maintain an inventory of SIM cards, failed to account for individuals to whom the SIM cards were registered, and allowed multiple employees to share login credentials on personal devices. The organisation had also exercised little or no supervision over their employees regarding how they used or accessed the customer's personal data.
- A financial penalty of S\$28,000 was imposed on Horizon Fast Ferry for failing to put in place reasonable security arrangements to protect its platform users' personal data in its possession or under its control. The organisation did not have its own IT department and relied informally on the goodwill of an employee of its overseas IT vendor to provide support. The organisation was found to have lacked basic IT security measures, including an ICT policy, vendor management protocols and security controls for its web server. It had no formal agreement with its IT vendor and failed to ensure that root account credentials were properly managed or deactivated after termination of service contracts. This resulted in the unauthorised access and exfiltration of users' personal data. The PDPC also noted this was not the organisation's first instance of non-compliance with the PDPA.
- A financial penalty of S\$74,000 was imposed on PPLingo for breaches of the Protection and Accountability Obligations. At the time of the incident, the organisation had in place a data protection policy and had implemented certain security measures for its platform, including network access control measures and firewall protection. The organisation also organised two rounds of awareness training for its IT development team one month before the incident. Nevertheless, given the high volume and sensitivity of the data, the onus was on the organisation to implement an appropriately robust level of security arrangements to satisfy the Protection Obligation. The PDPC found that the organisation had failed to put in place reasonable security arrangements to protect the personal data of over 557,000 users, including minors and individuals whose data included sensitive financial information. This included its failure to implement adequate password policies, such as mandating a minimum level of password complexity. The PDPC also noted that PPLingo had failed to appoint a Data Protection Officer since its incorporation in 2016, contrary to its obligations under the PDPA.

17.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

We have not sighted a published decision whereby the PDPC

has exercised its powers against companies established in other jurisdictions with no presence in or nexus to Singapore. That said, the PDPC investigated a company established overseas which collected the personal data of Singapore residents through a registered branch office (see, e.g. *Re Cigna Europe Insurance Company S.A.-N.V.* [2019] SGPDP18).

Nonetheless, the PDPC is empowered to enter into a co-operation agreement with a foreign data protection authority for data protection matters such as cross-border cooperation. Specifically, under Section 10 of the PDPA, cooperation agreements may be entered into for the purposes of:

- facilitating cooperation between the PDPC and another foreign data protection authority in the performance of their respective functions insofar as those functions relate to data protection; and
- avoiding duplication of activities by the PDPC and another foreign data protection authority, where those activities involve the enforcement of data protection laws.

The PDPC may also furnish information to a foreign data protection body pursuant to a cooperation agreement, subject to the fulfilment of certain prescribed conditions.

The PDPC is also a participant of the APEC Cross-Border Privacy Enforcement Arrangement, which creates a framework for the voluntary sharing of information and provision of assistance for privacy enforcement-related activities.

18 E-discovery/Disclosure to Foreign Law Enforcement Agencies

18.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Generally, organisations must ensure that any transfers of personal data outside of Singapore comply with the requirements under the PDPA (see our responses in section 12 above). It is not uncommon for Singapore businesses to include, in their privacy policy, a general notice that any personal data they collect may be disclosed to foreign law enforcement agencies or in relation to investigations and legal proceedings.

18.2 What guidance has/have the data protection authority(ies) issued on disclosure of personal data to foreign law enforcement or governmental bodies?

The PDPC has not issued any specific guidance yet in relation to the disclosure of personal data to foreign law enforcement or governmental bodies.

19 Artificial Intelligence

19.1 Are there any limitations on automated decision-making involving the processing of personal data using artificial intelligence?

The PDPA does not impose any specific limitations to automated decision-making that processes personal data in AI systems. However, where the automated decision-making system involves the collection, use or disclosure of personal data, the general Data Protection Provisions would apply.

19.2 What guidance (if any) has/have the data protection authority(ies) issued in relation to the processing of personal data in connection with artificial intelligence?

In its Advisory Guidelines on the Use of Personal Data in AI Recommendation and Decision Systems (issued on 1 March 2024), the PDPC highlighted that when organisations deploy AI systems in their services or products that collect, use or disclose personal data to provide new functionalities or to conduct automated decision-making, they should be mindful of the Consent (Sections 13 to 20 of the PDPA), Notification (Section 20 of the PDPA), and Accountability (Sections 11 and 12 of the PDPA) Obligations.

In particular, the Consent and Notification obligations under the PDPA operate in tandem to ensure that individuals are informed and their participation is meaningful. When organisations rely on AI systems to process personal data for decision-making purposes, they must inform individuals of the purposes of collection and intended uses of their data at the point of obtaining consent. This ensures that any consent provided is informed and meaningful.

The PDPC recommends that organisations provide, to the extent practicable:

- a clear explanation of the functionality of the product or service that relies on personal data;
- a general description of the types of data being collected and processed;
- details of how the data processing supports the product feature; and
- the specific data attributes that are likely to influence the AI output or decision.

Where organisations assess that it is necessary to limit the detail provided in favour of a more general explanation due to commercial sensitivity or security concerns over its AI systems, they are expected to document their justifications internally.

Furthermore, under the Accountability Obligation, organisations must be transparent in their use of AI systems. This includes maintaining internal policies and safeguards that promote fairness and reasonableness in how decisions are made. The depth of transparency expected is proportionate to the risks involved in each use case, such as the potential harm to individuals or the extent to which the AI system operates autonomously.

20 Trends and Developments

20.1 In your opinion, what enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.

Breaches of the Protection Obligation under the PDPA continue to constitute the majority of enforcement decisions issued by the PDPC, with the majority of cases over the past 12 months involving the Protection Obligation.

20.2 In your opinion, what “hot topics” are currently a focus for the data protection regulator?

New PDPC Guides Concerning Children’s Personal Data and AI

On 28 March 2024, the PDPC published the Children’s Personal Data Guidelines. Please see our response to question 6.1 for more information.

On 1 March 2024, the PDPC published its Advisory Guidelines on Use of Personal Data in AI Recommendation and Decision Systems. The guidelines provide guidance on how the PDPA applies when organisations use personal data to develop and train AI systems and set out best practices for how service providers (e.g. systems integrators) may support organisations implementing bespoke or fully customisable AI systems.

New and Updated ASEAN Guides

On 2 February 2024, during the 4th ASEAN Digital Ministers’ Meeting, the ASEAN Guide on AI Governance and Ethics (“**ASEAN AI Guide**”) and the updated Joint Guide to ASEAN MCCs and EU SCCs were launched. The ASEAN AI Guide sets out common principles for trustworthy AI and best practices for implementation in ASEAN. Please see our response to question 12.6 regarding the updated Joint Guide to ASEAN MCCs and EU SCCs.

At the 5th ASEAN Digital Ministers’ Meeting held in Bangkok, Thailand, on 16 to 17 January 2025, several initiatives were introduced to enhance the regulation and facilitation of cross-border data flows:

- A Joint Guide comparing the ASEAN MCCs with the Ibero-American Data Protection Network (“**RIPD**”) MCCs was published. It aims to help businesses, particularly companies already familiar with the ASEAN MCCs, to navigate contractual negotiations for international data transfers with their RIPD business partners.
- The ASEAN–China 2025 Digital Work Plan was endorsed, featuring a Joint Guide that maps ASEAN MCCs against China’s Standard Contractual Clauses for cross-border data flows. While not legally binding, these guides are expected to aid multinational businesses in understanding the interplay between various regional frameworks, thereby easing compliance.
- The meeting acknowledged the efforts of the ASEAN Working Group on Digital Data Governance in advancing the use and interoperability of ASEAN MCCs, including its collaboration with the Ibero-American Data Protection Network. It also welcomed the Operational Framework for Global CBPR and PRP, and encouraged ASEAN Member States to adopt these certification systems to promote trust, support cross-border data movement and bolster the regional digital economy.



Lim Chong Kin is the Managing Director of Drew & Napier's Corporate & Finance department and co-heads the Data Protection, Privacy & Cybersecurity Practice and the Competition Law & Regulatory Practice. He also heads the Telecommunications, Media and Technology ("TMT") Practice.

Chong Kin is a pioneer in the field of data protection in Singapore. His work in data protection, privacy and cybersecurity in Drew & Napier precedes the advent of Singapore's Personal Data Protection Act 2012 and Cybersecurity Act 2018. His expertise extends beyond general data protection law to sectoral frameworks, in particular, in the TMT and emerging AI sectors. Under Chong Kin's leadership, Drew & Napier has been recognised as one of the world's top 100 data law firms in *Global Data Review (GDR 100)*. Our TMT Practice Group has also been consistently ranked as the leading information technology, telecommunications, broadcasting and multimedia legal practice in Singapore. His clients include data protection regulators, MNCs driving the data world, and many global technology clients. Chong Kin's private sector experience includes advising corporations on their data protection compliance programmes, policies and practices, data breach management and cross-border data transfers (including in relation to transfer impact assessments). Chong Kin and his team have also advised clients on sectoral data protection requirements for many years, including that under TMT, financial and healthcare sectoral laws.

Chong Kin established the Drew Data Protection and Cybersecurity Academy (<https://www.drewnapier.com/Data-Protection-Cybersecurity-Academy>) in 2020, a first of its kind which offers clients value-add services including training and external DPO services.

Chong Kin has consistently been cited as a leading lawyer by *Chambers Asia Pacific*, *Asia Pacific Legal 500*, *Asialaw Profiles*, *PLC Which Lawyer?*, *International Who's Who of Regulatory Communications Lawyers*, *Best Lawyers* and *Asialaw Leading Lawyers*.

Chong Kin has also been recognised as a Senior Accredited Specialist in Data and Digital Economy Law by the Singapore Academy of Law.

Drew & Napier LLC

10 Collyer Quay
10th Floor Ocean Financial Centre
Singapore 049315

Tel: +65 6531 4110
Email: chongkin.lim@drewnapier.com
LinkedIn: www.linkedin.com/in/chong-kin-lim



Anastasia Su-Anne Chen is a Director with the Corporate & Finance Department in Drew & Napier. Her key areas of practice are TMT, Data Protection, Privacy and Cybersecurity. Prior to joining the firm, Anastasia was Deputy Chief Counsel to Singapore's Personal Data Protection Commission (PDPC) and Info-communications Media Development Authority (IMDA) for over nine years. She was lead counsel for PDPC matters, IMDA procurement and intellectual property portfolios, as well as the legal advisor to IMDA's Data Administration Group. During her stint with the public sector, she advised on numerous significant national projects, including overseeing major revisions to the PDPA, which came into effect on 1 February 2021.

Anastasia has advised on a broad range of regulatory, compliance and commercial matters. Her extensive experience ranges from implementing data protection compliance programmes, developing playbooks and contractual clauses for novel areas such as AI (including for world-leading Generative AI platforms), as well as providing strategic advice on international data flows, the outsourcing of data processing and data incidents.

Anastasia has been recognised as a Senior Accredited Specialist in Data & Digital Economy Law by the Singapore Academy of Law. She has also received several accolades for her data and cybersecurity practice, with clients commending her deep industry and regulatory experience, ability to anticipate potential legal issues, and subject matter expertise especially when dealing with novel problems.

Anastasia speaks regularly at data protection conferences and corporate events on data privacy. She was also an editor for the *Personal Data Protection Digests* for Singapore and has penned several articles contributing to the jurisprudence on data protection in Singapore.

Drew & Napier LLC

10 Collyer Quay
10th Floor Ocean Financial Centre
Singapore 049315

Tel: +65 6531 4123
Email: anastasia.chen@drewnapier.com
LinkedIn: www.linkedin.com/in/anastasiasuannechen

Drew & Napier established a dedicated Data Protection, Privacy and Cybersecurity Practice (<https://www.drewnapier.com/Our-Expertise/Data-Protection-Privacy-Cybersecurity>) to leverage its unrivalled experience in data privacy and data and cyber governance and offer clients best-in-class solutions to address their legal and compliance needs in Singapore and across the region. Our expertise covers the full range of regulatory, commercial and global aspects of data protection and cybersecurity and, working in tandem with the Drew Data Protection & Cybersecurity Academy (<https://www.drewnapier.com/Academy>), we seek to address our clients' needs with an integrated and holistic approach.

The Practice Group is headed by Directors Lim Chong Kin and David N. Alfred and the team includes professionals with deep technical expertise and a solid understanding of corporate governance and business needs in relation to data protection and cybersecurity.

A distinguishing feature of the practice is our in-house expertise on cybersecurity engineering, headed by a senior cybersecurity and privacy

engineer, Albert Pichlmaier, who has more than 30 years of experience. This enables the team to deliver a holistic solution to clients on data protection and cybersecurity compliance.

Our experience in data protection, privacy and cybersecurity predates, and also extends beyond, Singapore's Personal Data Protection Act 2012 (PDPA) and Cybersecurity Act 2018.

www.drewnapier.com

 **DREW & NAPIER**

Switzerland

FABIAN PRIVACY LEGAL GmbH



Daniela Fábán

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

In Switzerland, there is data protection legislation at federal and cantonal levels. The processing of personal data by private persons and federal bodies is governed by the Federal Act on Data Protection of September 25, 2020 (FADP) and the associated ordinances. The processing of personal data by cantonal and communal authorities is governed by cantonal data protection laws.

1.2 Is there any other general legislation that impacts data protection?

The FADP is complemented by the Ordinance on Data Protection and the Ordinance on Data Protection Certification. The Federal Act on Information Security also impacts data protection, but only applies to federal authorities and operators of critical infrastructure. The Federal Act on Unfair Competition (UCA) contains regulations regarding direct marketing, while the Telecommunications Act (TCA) regulates the use of cookies.

1.3 Is there any sector-specific legislation that impacts data protection?

There are various sector-specific laws that contain regulations regarding data protection, for example, in the medical sector (covering areas such as electronic patient records, research involving human beings, etc.), in the financial sector (e.g., banking and financial institutions' secrecy), etc.

1.4 What authority(ies) are responsible for data protection?

The Federal Data Protection and Information Commissioner (FDPIC) is the federal authority for overseeing the application of the FADP. Cantonal data protection laws are overseen by cantonal data protection authorities.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **“Personal data”**
Any information relating to an identified or identifiable natural person.
- **“Processing”**
Any handling of personal data, irrespective of the means and procedures used, in particular the collection, storage, keeping, use, modification, disclosure, archiving, deletion or destruction of data.
- **“Controller”**
A private person or federal body that, alone or jointly with others, determines the purpose and the means of processing personal data.
- **“Processor”**
A private person or federal body that processes personal data on behalf of the controller.
- **“Data subject”**
A natural person whose personal data is processed.
- **“Sensitive personal data”**
Data relating to religious, philosophical, political or trade union-related views or activities; data relating to health, the private sphere or affiliation to a race or ethnicity; genetic data; biometric data that uniquely identifies a natural person; data relating to administrative and criminal proceedings or sanctions; and data relating to social assistance measures.
- **“Breach of data security”**
A breach of security that leads to the accidental or unlawful loss, deletion, destruction, modification or unauthorised disclosure or access to personal data.
- **“Disclosure”**
Transmitting personal data or making such data accessible.
- **“Profiling”**
Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
- **“High-risk profiling”**
Profiling that poses a high risk to the data subject's personality or fundamental rights by matching data that

allows an assessment to be made of essential aspects of the personality of a natural person.

- **“Federal body”**

An authority or service of the Confederation or a person entrusted to carry out public tasks on behalf of the Confederation.

3 Territorial and Material Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The FADP applies to circumstances that have an effect in Switzerland, even if they are initiated abroad.

3.2 Do the data protection laws in your jurisdiction carve out certain processing activities from their material scope?

The FADP does not apply to personal data processing: (a) by a natural person exclusively for personal use; (b) by the Federal Assembly and parliamentary committees as part of their deliberations; and (c) by institutional beneficiaries who enjoy immunity from jurisdiction in Switzerland.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**

When collecting personal data, the controller must provide data subjects with adequate information to exercise their rights and ensure transparent data processing, at least the following information: (a) controller's identity and contact details; (b) purpose of processing; (c) if applicable, the recipients or categories of recipients of the personal data; (d) if the data is not collected from the data subject, the categories of processed personal data; and (e) if the personal data is disclosed abroad, the state or international body to which it is disclosed and the applicable guarantees or exception.

- **Lawful basis for processing**

Personal data must be processed lawfully. However, private controllers do not need a legal ground for processing, unless they process personal data contrary to the key principles or to the express wishes of the data subject, or disclose sensitive personal data to third parties. In these cases, the processing must be justified by the consent of the data subject, an overriding private or public interest or by law. Federal bodies may only process personal data if there is a statutory basis for doing so.

- **Purpose limitation**

Personal data may only be collected for a specific purpose that the data subject can recognise and may only be further processed in a manner that is compatible with this purpose.

- **Data minimisation**

Data minimisation is implied in the principle of proportionality.

- **Proportionality**

Data processing is proportionate if the data is necessary and suitable to achieve the intended purpose.

- **Retention**

Personal data must be destroyed or anonymised as soon as it is no longer required for the purpose of processing.

- **Accuracy**

Whoever processes personal data must make sure that the data is accurate and take all appropriate measures to correct, delete or destroy data that is incorrect or incomplete with respect to the purpose for which it is collected or processed.

- **Data security**

The controller and the processor must guarantee a level of data security appropriate to the risk by taking suitable technical and organisational measures.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

The FADP grants the data subject individual rights that can be asserted directly against the controller (e.g., the right of access and the right to data portability). In addition, the data subject can assert legal claims in court (e.g., request the rectification, erasure or destruction of data, prohibition of processing and disclosure to a third party).

- **Right of access to (copies of) data/information about processing**

Any person has the right to request information from the controller on whether personal data relating to them is processed and to receive the information required to be able to exercise their privacy rights and to guarantee transparent data processing. The right of access includes, among other information, information about the processed data as such. However, there is no right to receive a copy of the documents containing this information.

The controller may refuse to provide information if a formal law so provides, in particular, to preserve professional secrecy, to safeguard overriding third-party interests, or if the request is obviously unjustified or clearly frivolous.

- **Right to rectification of errors**

Data subjects have the right to request that incorrect personal data be corrected, unless a statutory provision prohibits the correction, or the personal data is processed for archiving purposes in the public interest.

- **Right to deletion/right to be forgotten**

Data subjects may request that personal data be deleted or destroyed.

- **Right to object to processing**

Data subjects have a right to request that their personal data not be processed. In this case, the data may only be processed if justified by an overriding private or public interest or by the law.

- **Right to request prohibition of processing**

Data subjects have a right to request that a specific data processing activity be prohibited.

- **Right to restrict processing**

If neither the accuracy nor the inaccuracy of the relevant personal data can be established, data subjects may request that the data be marked as being disputed.

- **Right to data portability**

Data subjects may request the controller to deliver to

them or, if no disproportionate effort is required, to transfer to another controller the personal data they have disclosed to it. The data must be delivered in a conventional electronic format, and, as a rule, free of charge.

- **Right to withdraw consent**
Data subjects have the right to withdraw their consent at any time.
- **Right to object to marketing**
Data subjects have the right to object to marketing at any time and they must be offered a free and simple way to object to further marketing (opt-out) in each marketing communication, usually by providing a link to unsubscribe.
- **Right protecting against solely automated decision-making and profiling**
Data subjects have the right to express their point of view and to request that the automated decision be reviewed by a natural person.
- **Right to complain to the relevant data protection authority(ies)**
Data subjects have the right to file a report on possible data protection violations with the competent data protection authority.
- **Right to object to the disclosure of personal data**
Data subjects may request that a specific disclosure of personal data to third parties be prohibited.

5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

In principle, only the data subjects themselves can assert their rights under the FADP in court. Such proceedings are governed by the Swiss Code of Civil Procedure, which does not provide for collective redress.

However, not-for-profit organisations or associations can file a lawsuit in their own name to assert violations of their members' personality rights, provided their articles of association permit this.

6 Children's Personal Data

6.1 What additional obligations apply to the processing of children's personal data?

With regard to consent, the general provisions of the Swiss Civil Code apply, which regulate the capacity of judgment for the validity of the consent of a minor. In the case of data processing to check creditworthiness based on a legitimate interest, the data subject must be at least 18 years old.

7 Registration Formalities and Prior Approval

7.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

There is no registration or notification obligation for private controllers. Federal bodies must notify their processing activities to the FDPIC.

7.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

The registration must be specific and list all processing activities as well as all mandatory information (cf. question 7.5).

7.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

Registrations are made per federal body and per processing activity.

7.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

Only federal bodies must register their processing activities.

7.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

The following information is mandatory: identity of the federal body; designation of the processing activity; purpose of processing; categories of personal data processed; categories of recipients; categories of data subjects; retention period; description of TOMs; legal basis; and in case of cross-border data transfer, destination countries and applicable guarantees.

7.6 What are the sanctions for failure to register/notify where required?

The FADP does not provide for sanctions for failure to register/notify.

7.7 What is the fee per registration/notification (if applicable)?

There is no fee.

7.8 How frequently must registrations/notifications be renewed (if applicable)?

The law does not provide for a regular review, but registrations must be kept up to date and amended in case of changes.

7.9 Is any prior approval required from the data protection regulator?

General prior approval is not required. However, for processing activities that are likely to result in a high risk to a data subject's personality or fundamental rights, a data protection impact assessment (DPIA) must be carried out. If the residual risk is still high, despite the measures taken, the

DPIA must be submitted to the FDPIC for an opinion, except for private controllers who have appointed a Data Protection Officer (DPO).

7.10 Can the registration/notification be completed online?

Yes, it must be completed online on the portal of the FDPIC (<https://www.datareg.edoeb.admin.ch>).

7.11 Is there a publicly available list of completed registrations/notifications?

The portal of the FDPIC is public and all active registrations can be viewed by anyone.

7.12 How long does a typical registration/notification process take?

The registration process is completed directly online.

8 Appointment of a Data Protection Officer

8.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

Federal bodies must appoint a DPO. For private controllers, the appointment of a DPO is voluntary.

8.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

The FADP does not provide for sanctions for failure to appoint a DPO.

8.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

There is no specific protection for DPOs; the general provisions of employment law apply.

8.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

Yes, this is permitted, also for federal bodies.

8.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The DPO must have the required expert knowledge, must exercise his or her function towards the controller in a professionally independent manner without being bound by instructions and must not carry out any activities that are incompatible with his or her tasks as a DPO.

8.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

The DPO provides support in applying the data protection regulations, trains and advises the controller and its employees on data protection matters and serves as a contact point for data subjects and data protection authorities.

8.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

Federal bodies must in any case notify the FDPIC; private controllers only if they wish to benefit from the exception to consult the FDPIC (cf. question 7.9).

8.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

Federal bodies must in any case publish the DPO's contact details; private controllers only if they wish to benefit from the exception to consult the FDPIC (cf. question 7.9).

9 Appointment of Processors

9.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes, unless the assignment is based on a legal provision, the processing may be contractually assigned to a processor if (a) the data is processed only in the manner in which the controller is permitted to do so, and (b) no legal or contractual confidentiality obligation prohibits the assignment.

9.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The FADP contains neither a list of items to be regulated in the agreement nor formal requirements. However, a written agreement is recommended obliging the processor to process the data as instructed by the controller, not to assign the processing to third parties without the prior authorisation of the controller and to ensure adequate data security.

10 Marketing

10.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

Unsolicited mass advertising through telecommunications (e.g., email, SMS, web messenger services) must comply with the UCA. Under this law, such advertising requires prior consent and correct indication of the sender, as well as an option for refusal. Consent can be inferred if the sender (a) has obtained the contact details directly from the recipient

in connection with a legal transaction, (b) has indicated the possibility of rejecting mass advertisement (opt-out), and (c) only sends advertising relating to its own similar products or services as the previously concluded legal transaction. The processing of personal data, (e.g., contact information, preferences) is subject to the data protection principles of the FADP.

10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

The UCA applies to both business-to-consumer and business-to-business marketing.

10.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

According to the UCA, telemarketing requires prior consultation of the telephone directory as a public opt-out register. If there is no entry in the directory or if an entry is marked with an asterisk (*) indicating that a customer does not wish to receive advertising from callers with whom they do not have a business relationship and that their data may not be passed on for the purposes of direct advertising, telephone marketing is considered unfair competition. Marketing by post is also subject to an opt-out rule. If a sign saying “No advertising please” is attached to a letterbox, marketing campaigns constitute a violation of the UCA.

10.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Yes. Both the UCA and the FADP apply to matters that have an effect in Switzerland, even if they were initiated abroad.

10.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

No, the State Secretariat for Economic Affairs and the cantonal prosecution authorities are responsible for enforcing the marketing restrictions laid down in the UCA.

10.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Yes, the trade of marketing lists is permitted if both the buyer and the seller comply with the applicable regulations (i.e., the FADP and UCA).

10.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Violations are subject to severe criminal sanctions. Wilful infringement of the applicable UCA provisions can be punished with imprisonment of up to three years or a fine. FADP violations are subject to a fine of up to CHF 250,000.

11 Cookies

11.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

The use of cookies and similar technologies in Switzerland is regulated by the TCA. Pursuant to Art. 45(c) TCA, opt-in consent is not required, provided that the users have been informed about the use of cookies and similar technologies and the related data processing and its purpose, and how they can be deactivated (opt-out principle).

When the use of cookies and similar technologies involves the processing of personal data, the requirements of the FADP must be complied with. As private controllers do not need a legal justification as long as the processing has a lawful purpose, is proportionate and carried out in good faith according to the statutory principles, consent is generally not required by law.

11.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

The current legislation does not distinguish between different types of cookies. However, in his guidelines on data processing by means of cookies and similar technologies, the FDPIC states that any use of non-essential cookies violates the principle of proportionality and therefore needs a legal justification. The FDPIC recommends obtaining consent for any use of non-essential cookies that is not generally expected by users and/or leads to profiling, such as web analysis, personalised advertisement, etc. Explicit consent is, according to the FDPIC, required when sensitive personal data is processed or in the case of high-risk profiling, e.g., cross-site tracking. These recommendations are not legally binding, but they can be an indicator for possible future areas of focus in investigations.

11.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

In his final report on the investigation into the Ricardo auction platform published in April 2024, the FDPIC concluded that Ricardo and its mother company TX Group were, contrary to their affirmations, processing personal data, particularly as the usage data was always linked to a unique pseudonym. He also found that the cross-platform tracking led to the creation of personality profiles (high-risk profiling under the new FADP) and that Ricardo members were not adequately informed about the tracking and the subsequent use of data for targeted advertising. According to the FDPIC, resulting breaches of privacy could not be justified by the overriding private interests that Ricardo and TX Group claimed, and valid consent was not obtained, not least because the users were not adequately informed about the data processing. The FDPIC therefore recommended that these deficiencies be remedied by making data transfers and cross-platform tracking transparent and by obtaining valid consent for these practices.

Ricardo and TX Group contested most of the FDPIC’s findings, and it is not clear at the time of writing what further measures will be taken by the parties. Nevertheless, the FDPIC’s opinion and recommendations emphasise the importance he attaches to this issue, and his restrictive interpretation of the law.

11.4 What are the maximum penalties for breaches of applicable cookie restrictions?

The maximum penalty can amount up to CHF 5,000 for a breach of the TCA or CHF 250,000 for a breach of the FADP (e.g., wilful provision of false or incomplete information or wilful failure to provide information to data subjects).

12 Restrictions on International Data Transfers

12.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Personal data may only be transferred abroad if the Federal Council has decided that the legislation of the respective state or international body guarantees an adequate level of protection. The list of adequacy decisions can be found in Annex 1 to the Ordinance on Data Protection. In the absence of an adequacy decision, personal data may only be transferred cross-border with additional guarantees or when one of the exceptions provided for by the FADP applies.

12.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

Businesses typically rely on the EU Standard Contractual Clauses (SCC) for transferring personal data to third countries without an adequacy decision. The FCPIC has recognised the SCC as a valid transfer mechanism, but requires some Swiss-specific adaptations, e.g., with respect to the competent supervisory authority, the applicable law for contractual claims, etc. Businesses may also rely on Binding Corporate Rules (BCR) for intragroup data transfers.

In addition, businesses may transfer personal data to third countries based on an exemption, the most relevant being: the data subject's explicit consent; disclosure directly connected with the conclusion or performance of a contract with the data subject or in the interests of the data subject; and disclosure necessary to safeguard an overriding public interest or to establish, exercise or enforce legal rights before a court or another competent foreign authority.

12.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

Federal bodies must document all cross-border data transfers in their register of processing activities, which is notified to the FDPIC (cf. question 7.5). If contractual clauses other than those approved by the FDPIC are used, they must be notified beforehand to the FDPIC.

12.4 Do transfers of personal data to other jurisdictions require a transfer impact assessment? If conducting a transfer impact assessment is only mandatory in some circumstances, please identify those circumstances.

A transfer impact assessment (TIA) is required for transfers based on SCC or other transfer mechanisms to countries without an adequate level of protection. The FDPIC has issued a guide to checking the admissibility of data transfers to foreign countries, first published in June 2021 and amended in May 2023. It lists four guarantees that should be evaluated in the course of a TIA, as well as mandatory supplemental measures if these guarantees are not met.

12.5 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?

The FDPIC ruled in September 2020 that the CH-US Privacy Shield does not provide an adequate level of data protection anymore. On 14 August 2024, the Federal Council recognised the Swiss-US Data Privacy Framework as offering an adequate level of data protection. Since 15 September 2024, personal data can thus be transferred to certified US companies without any additional safeguards.

12.6 What guidance (if any) has/have the data protection authority(ies) issued in relation to the use of standard contractual/model clauses as a mechanism for international data transfers?

The FCPIC has recognised the SCC as a valid transfer mechanism with some Swiss specifications, which are outlined in the FCPIC's guideline of August 2021 on data transfers based on standard data protection clauses (cf. question 12.2). In his amendment of 12 February 2025 to the aforementioned guideline, the FDPIC further recognised the Model Contractual Clauses for the Transfer of Personal Data (MCC) in accordance with Art. 14 para. 3 let. b of the modernised Council of Europe Convention 108 (C108), adopted by the Consultative Committee on C108 in June 2024, as a valid transfer mechanism.

13 Whistle-blower Hotlines

13.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

In Switzerland, there are laws that require the implementation of whistle-blower procedures, e.g., for the purpose of child labour prevention. These provisions do not legally restrict the type of issues that may be reported, the circle of persons who may submit a report or the persons whom a report may concern. However, the data processing in connection with whistle-blower hotlines must comply with the FADP and employment legislation.

13.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous reporting is permitted.

14 CCTV

14.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

No separate registration/notification or prior approval from the FDPIC is required for the use of video surveillance. However, the use of video surveillance must comply with Swiss labour law, which generally prohibits behavioural surveillance. The use of CCTV must also comply with data protection requirements, in particular the principles of legality, proportionality, data security and transparency. The persons concerned must be informed prior to video surveillance (e.g., by means of a visible sign).

14.2 Are there limits on the purposes for which CCTV data may be used?

Yes. Swiss labour law prohibits the use of video surveillance for the (sole) purpose of employee behaviour surveillance (cf. section 15 below). According to the FDPIC, CCTV is further prohibited if it undermines the privacy and informational self-determination of data subjects, such as the processing of video surveillance footage for comprehensive facial recognition in real time.

15 Employee Monitoring

15.1 What types of employee monitoring are permitted (if any), and in what circumstances?

The use of CCTV for the (sole) purpose of monitoring the behaviour of employees is prohibited under Swiss employment law. However, surveillance for other reasons, such as for security reasons or for the allocation of resources, would be permitted provided that the processing is proportionate to the purpose pursued and the employees concerned are informed in advance of the installation of such systems and their purposes.

15.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Employers may handle data concerning employees only to the extent that such data concerns the employees' suitability for their job or is necessary for the performance of the employment contract. Justified monitoring systems typically fall into this scope and, therefore, mostly do not require consent of the employees due to the employer's legitimate interest. In any case, the affected employees must be informed prior to the use of any employee monitoring. Such notification is mostly provided by the means of an (employee) privacy notice.

15.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

Employee representatives are entitled to timely and comprehensive information on all matters that they require for the proper representation of the employees' common interests *vis-à-vis* the employer. As employee monitoring systems affect employees' interest and are common reasons for conflicts, it is highly advised to inform employee representatives about such practices.

15.4 Are employers entitled to process information on an employee's attendance in office (e.g., to monitor compliance with any internal return-to-office policies)?

Swiss law takes a purpose-oriented approach to employee monitoring (cf. question 15.1). Information may be processed to safeguard legitimate business interests (i.e., the execution of the employment contract and thus, for example, the efficient allocation of personnel or the operation of office infrastructures on site), provided that the data protection requirements are met.

16 Data Security and Data Breach

16.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

The controller and the processor must take appropriate technical and organisational measures to ensure a level of data security appropriate to the risk.

16.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Yes. The controller must notify the FDPIC (via an online form) as quickly as possible of any data breach that may result in a high risk to the data subject's personality or fundamental rights.

The notification must include the following information: (a) form of breach; (b) time and duration, if possible; (c) categories and approximate amount of personal data concerned, if possible; (d) categories and approximate number of data subjects, if possible; (e) consequences, including any risks, for the data subjects; (f) measures that have been taken or are planned to remedy the breach and mitigate the consequences, including any risks; and (g) the name and contact details of a contact person.

16.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

The controller must inform the data subjects if this is required for their protection or if the FDPIC so requests. It may limit, delay or refrain from the notification to data subjects if: (a) this is required to safeguard overriding third-party interests; (b) the controller is a federal body and the measure is required to satisfy overriding public interests, or the notification may compromise an enquiry, an investigation or administrative or judicial proceedings; (c) the notification is impossible or requires disproportionate effort; or (d) the notification to the data subjects is equally guaranteed by a public announcement.

The following information must be provided: (a) form of breach; (b) consequences, including any risks, for the data subjects; (c) measures that have been taken or are planned to remedy the breach and mitigate the consequences, including any risks; and (d) the name and contact details of a contact person.

16.4 What are the maximum penalties for personal data security breaches?

The FADP does not provide for specific sanctions for data breaches or for failure to report a data breach to the FDPIC or to the individuals concerned, but failure to comply with the minimum requirements for data security and wilful disclosure of secret personal data are subject to a fine up to CHF 250,000.

17 Enforcement and Sanctions

17.1 Describe the enforcement powers of the data protection authority(ies).

- (a) **Investigative powers:** The FDPIC shall open an investigation *ex officio* or upon report of data subjects or third parties if there are sufficient indications that a data processing activity could violate data protection regulations. In the case of failure to cooperate, the FDPIC may order access to information, documents, premises and installations and is also entitled to conduct questioning of witnesses or to obtain appraisals by experts.
- (b) **Corrective powers:** If the FDPIC concludes that data protection regulations have been violated, he can *inter alia* order that the federal body or the private person (a) modifies, suspends or terminates the processing, wholly or in part, and deletes or destroys the personal data, wholly or in part, (b) delays or aborts a disclosure abroad, (c) implements measures to ensure data protection by design, data protection by default or data security requirements, (d) duly informs the data subjects in a manner that allows them to exercise their rights, (e) conducts a DPIA, (f) provides notifications on data security breaches, or (g) grants the right to information to data subjects.
- (c) **Authorisation and advisory powers:** The FDPIC advises federal bodies and private persons on data protection matters. He also develops and publishes working instruments as advisory for good practice for use by controllers,

processors and data subjects. The authorisation powers of the FDPIC are mainly found within the area of cross-border data disclosure, where the FDPIC has to approve standard data protection clauses or BCR if relied upon for transfers and as regards to DPIAs, where the FDPIC can raise objections to planned processing activities, if a DPIA indicates that a planned processing despite security measures still poses a high risk to the data subject's personality or fundamental rights.

- (d) **Imposition of administrative fines for infringements of specified legal provisions:** The FDPIC has no authority to impose administrative sanctions. However, if certain substantial obligations are wilfully violated, individuals can face criminal fines up to CHF 250,000 which are enforced by cantonal prosecution authorities. Violations that are subject to criminal charges include wilful provision of false or incomplete information on data processing, unlawful cross-border data transfers (e.g., without adequate guarantees), assignment to a processor in breach of applicable confidentiality duties or without guaranteeing data security and failure to comply with minimum data security standards outlined by the Swiss Federal Council. Note that, in contrast to the GDPR, these fines are directed against individuals and not legal entities. However, as an exception, the business can be fined if the amount would not exceed CHF 50,000 and the identification of the perpetrators would require disproportionate measures.
- (e) **Non-compliance with a data protection authority:** Fines not exceeding CHF 250,000 can be imposed on private persons (individuals) who provide the FDPIC with false information or wilfully fail to cooperate during an investigation.

17.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The FDPIC has the power to inhibit a particular processing activity without a court order. However, the imposed ban can be appealed to the Federal Administrative Court.

17.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

As the revised FADP granting the FDPIC extended powers only entered into force in September 2023, there have not been many cases yet under the revised law. According to the FDPIC's publication "*The new data protection act in figures*" dated 18 November 2024, the FDPIC opened 26 preliminary enquiries and investigations under the new law, of which seven had been concluded at the time of issuing the report. As an example, the investigation into Bürgerforum Schweiz can be cited. This association sent out questionnaires to persons working in the church environment regarding their religious beliefs, published the answers on a publicly accessible website without the data subjects' consent and refused to comply with data subjects' deletion requests, invoking an overriding public interest. The FDPIC carried out an investigation and ordered Bürgerforum Schweiz to only publish the responses of persons who had expressly consented and to comply with deletion requests.

17.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

The FADP is subject to the principle of impact (*cf.* question 3.1), which enables proceedings against companies based in other jurisdictions if data processing has an impact in Switzerland. Judicial decisions against companies outside Switzerland are enforced via formal international enforcement proceedings. The FDPIC further has the power to open investigations against companies located outside Switzerland, which he did, for example, in his recently concluded preliminary investigation into the use of personal data for training the artificial intelligence (AI) Grok by the operator of the platform X, Twitter International Unlimited Company.

18 E-discovery/Disclosure to Foreign Law Enforcement Agencies

18.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

When companies in Switzerland are confronted with foreign e-discovery or data disclosure requests, they must consider both the Swiss Criminal Code, which prohibits taking or facilitating actions by a foreign state on Swiss territory without lawful authority, and the FADP. Foreign requests transmitted through formal legal channels can be fulfilled in accordance with the principles of data protection, most relevant are data minimisation, data security and the requirements for lawful cross-border transfers.

18.2 What guidance has/have the data protection authority(ies) issued on disclosure of personal data to foreign law enforcement or governmental bodies?

The FDPIC has not issued guidance on this specific topic. However, general guidance on cross-border data transfers and on access to employees' data (e.g., emails) are relevant.

19 Artificial Intelligence

19.1 Are there any limitations on automated decision-making involving the processing of personal data using artificial intelligence?

Pursuant to Art. 21 FADP, the controller must inform the data subject about any decision that is based exclusively on automated processing and that has a legal consequence for or a considerable adverse effect on the data subject (automated individual decision). Data subjects have the right to express their point of view and to request that the decision be reviewed by a natural person. This applies to any automated individual decisions, whether AI is involved or not. As Switzerland has not introduced specific AI legislation yet, there are no particular regulations for automated decision-making using AI.

19.2 What guidance (if any) has/have the data protection authority(ies) issued in relation to the processing of personal data in connection with artificial intelligence?

In a statement published in November 2023, the FDPIC pointed out that the FADP is directly applicable to the use of AI-supported data processing, and drew particular attention to the data subjects' right to privacy and informational self-determination and to the transparency requirements.

20 Trends and Developments

20.1 In your opinion, what enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.

Since the entry into force of the revised FADP in September 2023, the FDPIC issued a number of guides, factsheets, templates, etc. and updated existing documents to reflect the new legislation. Particular focus was put on technical issues such as technical and organisational measures, the use of cookies, data security breaches, etc. In particular, in his guideline on the use of cookies and similar technologies, the FDPIC adopted a very restrictive view that goes beyond the statutory requirements. Even if these guidelines are not legally binding, they can be considered an indicator of possible future areas of focus in investigations.

Investigations recently concluded by the FDPIC concerned, among others, data security breaches and processing by processors, for example in the investigation into the Federal Office of Police, the Federal Office for Customs and Border Security and their IT service provider and processor Xplain, who was subject to a ransomware attack, as a consequence of which a large volume of personal data originating from the Federal Offices and stored on Xplain's servers was published on the darknet. Other areas of focus were the principles of transparency and proportionality and the concept of personal data. As examples, the investigations into the data processing practices of one of Switzerland's largest online retailers, Digitec Galaxus, as well as the auction platform Ricardo and its mother company TX Group, may be cited (*cf.* question 11.3). Although these investigations were initiated under the former law, they give an indication of the FDPIC's enforcement priorities.

20.2 In your opinion, what "hot topics" are currently a focus for the data protection regulator?

An important topic in Switzerland is currently AI regulation. On 27 March 2025, Switzerland signed the Council of Europe Convention on Artificial Intelligence and thus committed itself to making the necessary amendments to Swiss law, with the objective of strengthening Switzerland as a location for business and innovation while keeping the risks to society as low as possible. This shall be achieved by implementing general, cross-sectoral legislation for state actors, and, in key areas such as data protection, that shall be complemented by sector-specific regulations and additional, legally non-binding measures. A draft bill and a plan for additional measures are expected by the end of 2026.



Daniela Fábíán is the founder and executive director of FABIAN PRIVACY LEGAL GmbH.

Daniela has more than 30 years of experience in data protection, employment law, risk and programme management, security and related areas, including 19 years in-house. She advises multinational companies, SMEs and start-ups from various industries, mainly in the EU, Switzerland and the US, on data, data protection, AI, security and related issues, particularly in the life sciences, pharmaceutical and medical technology sectors.

Daniela supports her clients in the assessment, development, implementation and monitoring of data and privacy strategies, data, privacy, and AI governance models and global data protection and AI programmes, as well as data transfer mechanisms with a pragmatic approach. She advises her clients on technology and IT issues, digitalisation strategies, AI and data governance, outsourcing projects, data protection and cybersecurity, in particular on prevention, as well as on the creation and implementation of data incident response plans.

Daniela is a member of various data protection associations, the founder and chair of a Privacy Expert Roundtable (Life Sciences) in Switzerland and a lecturer at FernUni Switzerland for the CAS Data Protection and at the Swiss Health Quality Association for Digital Marketing.

FABIAN PRIVACY LEGAL GmbH

Bäumleingasse 10
4051 Basel
Switzerland

Tel: +41 61 544 44 01

Email: daniela.fabian@privacylegal.ch

LinkedIn: www.linkedin.com/in/daniela-fabian-masoch-106b67a

FABIAN PRIVACY LEGAL GmbH is a boutique law firm specialising in privacy and data protection laws and related issues, information security, data, AI and privacy governance, risk management, programme implementation and legal compliance.

Our strengths are the combination of expert knowledge and practical in-house experience, a strong network with industry groups and privacy associations, and close cooperation with experts in data protection, cybersecurity and cybercrime, in jurisdictions around the world. We approach mandates with a global, solution-oriented and practical approach, to deliver pragmatic and sustainable solutions.

www.privacylegal.ch



Taiwan



Yvonne Y.F. Lin



Jeffrey K.S. Hung



Jackie Yang

Formosan Brothers Attorneys-at-Law

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The Personal Data Protection Act (“PDPA”).

1.2 Is there any other general legislation that impacts data protection?

The Enforcement Rules of the Personal Data Protection Act (“Enforcement Rules of the PDPA”).

1.3 Is there any sector-specific legislation that impacts data protection?

Depending on the specific sector, the competent authority may request the company to establish a security and maintenance plan for the protection of personal data files and rules on disposing personal data following a business termination via regulations.¹

1.4 What authority(ies) are responsible for data protection?

Prior to the official assumption of responsibilities by the Personal Data Protection Commission,² the Preparatory Office of the Personal Data Protection Commission is actively engaged in laying the groundwork for its establishment. In the interim, various competent authorities, each designated by their respective industry sectors, are managing all matters related to data protection.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **“Personal Data”**
This refers to a natural person’s name, date of birth, national identification card number, passport number, physical characteristics, fingerprints, marital status, family information, education background, occupation, medical records, healthcare data, genetic data, sex life, records of physical examination, criminal records, contact information, financial conditions, social

activities and any other information that may be used to directly or indirectly identify a natural person.³

- **“Processing”**
This refers to the act of recording, inputting, storing, compiling/editing, correcting, duplicating, retrieving, deleting, outputting, connecting or internally transferring data for the purpose of establishing or using a personal data file.⁴
- **“Controller”**
This is not explicitly defined in the PDPA.
- **“Processor”**
Though not explicitly defined in the PDPA, the closest defined entity may be the commissioned legal person, group or natural person who collects, processes or uses personal data.⁵
- **“Data Subject”**
This refers to an individual whose personal data is collected, processed or used.⁶
- **“Sensitive Personal Data”/“Special Categories of Personal Data”**
This refers to data pertaining to a natural person’s medical records, healthcare, genetics, sex life, physical examination and criminal records.⁷
- **“Data Breach”**
This is not explicitly defined in the PDPA.
- **Other key definitions:**
 - **“Person”/“Individual”** refers to a living natural person.⁸
 - **“Indirectly Identified”** refers to the circumstances where a government or non-government agency possessing such data cannot directly identify the data subject, unless it compares, combines or connects such data with other data.⁹
 - **“Personal Data File”** refers to a collection of personal data structured to facilitate data retrieval and management by automated or non-automated means¹⁰ and includes the backup file(s).¹¹
 - **“Collection”** refers to the act of collecting personal data in any way.¹²
 - **“Use”** refers to the act of using personal data via any methods other than processing.¹³
 - **“Deleting”** refers to erasing the personal data from the personal data file.¹⁴
 - **“Internally Transferring”** refers to data transfer within a government or non-government agency.¹⁵
 - **“Medical Records”** refers to the data specified in the subparagraphs of Paragraph 2 of Article 67 of the Medical Care Act.¹⁶
 - **“Healthcare Data”** refers to medical histories and any other data pertaining to checkups or treatments

implemented by physicians or other medical professionals for the purpose of treating, correcting or preventing diseases, harms or disabilities of the human body or for other legitimate medical reasons, or shall mean other data produced from the prescription, medication, operation or disposition based on the findings of the above-mentioned checkups.¹⁷

- **“Genetic Data”** refers to the information on a heredity unit, consisting of one segment of DNA of the human body, for controlling the specific functions thereof.¹⁸
- **“Sex Life”** refers to the personal data on sexual orientation or sexual habits.¹⁹
- **“Records Of Physical Examination”** refers to the data produced by medical examinations conducted not for the purpose of diagnosing or treating a specific disease.²⁰
- **“Criminal Records”** refers to the records of deferred prosecutions, *ex officio* non-indictments, or a final guilty verdict rendered by a court and its enforcement.²¹

3 Territorial and Material Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

Yes. The PDPA also applies to the government and the non-government agencies outside the territory of Taiwan when they collect, process or use the personal data of Taiwan nationals.²²

3.2 Do the data protection laws in your jurisdiction carve out certain processing activities from their material scope?

Yes. The PDPA does not apply to the following circumstances:

1. where personal data is being collected, processed, or used by a natural person purely for purposes of personal or household activities; or
2. where audio-visual data is collected, processed, or used in public places or public activities and not connected to other personal data.²³

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**

If the collection or processing of personal data is based on the data subject's consent, the data subject shall be informed of the information required under the PDPA prior to giving a declaration of agreement.²⁴

If the use of personal data exceeds the necessary scope of the specific purpose of collection (for another purpose) and is based on the data subject's consent, the data subject shall be informed of any of the purposes other than that originally specified, the scope of other use, and the impact of giving or not giving consent on the rights and interests of the data subject prior to giving a separate declaration of agreement.²⁵

If any personal data is stolen, disclosed, altered or otherwise infringed upon due to a violation of the PDPA by a government or non-government agency, the data subject shall be notified via appropriate means after the relevant facts have been clarified.²⁶

- **Lawful basis for processing**

1. where it is expressly required by law;
2. where there is a contractual or quasi-contractual relationship between the non-government agency and the data subject, and proper security measures have been adopted to ensure the security of the personal data;
3. where the personal data has been manifestly made public by the data subject or publicised legally;
4. where it is necessary for statistics gathering or academic research by an academic institution in pursuit of public interests, provided that such data, as processed by the data provider or as disclosed by the data collector, may not lead to the identification of a specific data subject;
5. where consent has been given by the data subject;
6. where it is necessary for furthering public interests;
7. where the personal data is obtained from publicly available sources unless the data subject has an overriding interest in prohibiting the processing or use of such personal data; or
8. where the rights and interests of the data subject will not be infringed upon.²⁷

- **Purpose limitation**

The purposes of processing personal data must be specified, but there is no explicit limitation of such purposes in the PDPA.²⁸

- **Data minimisation**

The processing of personal data must not exceed the necessary scope of specific purposes.²⁹

- **Proportionality**

The processing of personal data must not exceed the necessary scope of specific purposes.³⁰

- **Retention**

This is not explicitly outlined in the PDPA, but for certain industries that have active regulations for the security and maintenance of personal information files in place, it is usually required to retain records associated with personal data usage, tracking logs or relevant evidence for at least five years. Should any laws or regulations prescribe a longer retention timeframe, that longer duration will be applicable.

- **Accuracy**

A data subject is entitled to request to supplement or correct his/her personal data.³¹

- **Honest and good faith**

The collection, processing and use of personal data must be carried out in a way that respects the data subject's rights and interest, in an honest and good-faith manner, must not exceed the necessary scope of specific purposes, and must have legitimate and reasonable connections with the purposes of collection.³²

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to (copies of) data/information about processing**

A data subject is entitled to request to make an inquiry of and to review his/her personal data.³³

- **Right to rectification of errors**
A data subject is entitled to request to supplement or correct his/her personal data.³⁴
- **Right to deletion/right to be forgotten**
A data subject is entitled to request to erase his/her personal data.³⁵
- **Right to object to processing**
A data subject is entitled to request to cease the processing of his/her personal data.³⁶
- **Right to restrict processing**
The right to information privacy ensures that individuals have the ability to exercise control over their personal data before it is used, as well as to oversee its use both during and after the use. This right to post-use control also includes the option to request the deletion, suspension or restriction of personal data usage.³⁷ (The distinction between “processing” and “use” in the PDPA is not obvious.)
- **Right to data portability**
Upon the request of a data subject, the government or non-government agency must reply to the data subject’s inquiry, allow the data subject to review the personal data collected, or provide the data subject with a copy thereof.³⁸
- **Right to withdraw consent**
If personal data is processed based on the consent of the data subject and that consent is later withdrawn, the processor must, from the moment of withdrawal, erase, stop processing, or refrain from using the personal data, unless otherwise specified in the exception outlined in Article 11, Paragraph 3 of the PDPA.³⁹
- **Right to object to marketing**
When a non-government agency uses personal data for marketing purposes (which is not within the necessary scope of the specific purpose of collection), upon the data subject’s objection to such use, the agency shall cease using the data subject’s personal data for marketing.⁴⁰
Non-government agencies, when using the data subject’s personal data for marketing purposes for the first time, must provide the data subject with ways that he/she can object to such use, and the agency must pay for the fees therefrom.⁴¹
- **Right protecting against solely automated decision-making and profiling**
This is not explicitly outlined in the PDPA.
- **Right to complain to the relevant data protection authority(ies)**
The data subject may file complaints to the relevant data protection authority(ies).
- **Right to compensation**
Non-government agencies shall be liable for the damages arising from any injury caused by any unlawful collection, processing or use of personal data, or other infringement on the rights of data subjects due to such non-government agency’s violation of the PDPA, unless the non-government agency can prove that such injury is not caused by its wilful act or negligence.⁴²

5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

Yes. Data subjects may mandate an incorporated foundation or an incorporated charity that brings a case to the court under certain circumstances.⁴³

6 Children’s Personal Data

6.1 What additional obligations apply to the processing of children’s personal data?

Children’s personal data must not be revealed to the media, or in publicly available information. This includes names or other details that are sufficient to identify children and youth that were involved in certain crimes, or materials that are harmful to their health, related parties of family law dispute, victims of juvenile delinquency, etc.⁴⁴

For data subject’s (informed) consent of minors, the language and terminology used must be comprehensible to them, and the consent may be subject to the approval of the minor’s legal guardian if necessary in accordance with the Civil Code.⁴⁵

7 Registration Formalities and Prior Approval

7.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

There is no general obligation, but for human biobanks, the biobank operator must apply to the competent authority for a permit.⁴⁶

7.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

It must be specific.⁴⁷

7.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

Per database and per biobank operator.

7.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

The human biobank operator.

7.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

The information must include: the types, quantities, and related data and information of biological specimens planned to be collected and preserved; the operating procedures for dealing with biological specimens and related data and information; the management provisions for information security; the contents of informed consent and the measures of participants’ rights

and interests protection; and the rules of notification mechanisms and remedies applicable when participants' biological specimens or related data and information are stolen, leaked, altered or suffer from other violations, among others.⁴⁸

7.6 What are the sanctions for failure to register/notify where required?

A fine of no less than NT\$2 million and no more than NT\$10 million.⁴⁹

7.7 What is the fee per registration/notification (if applicable)?

NT\$150,000 for a permit application.

7.8 How frequently must registrations/notifications be renewed (if applicable)?

The operator should submit the requested documents and data to the competent authority to apply for an extension to the permission certificate for setting up the biobank six months before the expiration of the valid period. Each extension is limited to three years.⁵⁰

7.9 Is any prior approval required from the data protection regulator?

Yes. The approval of the permit is required from the Ministry of Health and Welfare.

7.10 Can the registration/notification be completed online?

No, it cannot.

7.11 Is there a publicly available list of completed registrations/notifications?

Yes, there is.⁵¹

7.12 How long does a typical registration/notification process take?

This is not applicable.

8 Appointment of a Data Protection Officer

8.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The PDPA only requires the agency to allocate management of personnel and reasonable resources as the technical or organisational measures taken by a government agency or non-government agency for the purpose of preventing personal data from being stolen, altered, damaged, destroyed or disclosed.⁵² For certain industries that have active regulations for the security and maintenance of personal information

files in place, it is usually required that the enterprise assign a designated individual to manage the safety maintenance plan, who will be responsible for its planning, formulation, revision and implementation, along with other pertinent issues.

8.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

There are none.

8.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

This is not explicitly outlined in the PDPA.

8.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

Yes, it may.

8.5 Please describe any specific qualifications for the Data Protection Officer required by law.

This is not explicitly outlined in the PDPA or the current legal framework.

8.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

This is not explicitly outlined in the PDPA or the current legal framework.

8.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

No, this is not required.

8.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

No, this is not required.

9 Appointment of Processors

9.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

No, this is not required.

9.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

This is not applicable.

10 Marketing

10.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

The general provisions outlined in question 5.1 (Right to object to marketing) also apply to electronic direct marketing.

10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

These restrictions are only applicable to business-to-consumer marketing, as only a “natural person” can possess personal data as defined by the PDPA.

10.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

None. The same restrictions as outlined in question 5.1 (Right to object to marketing) shall apply.

10.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Yes. The PDPA also applies to entities outside Taiwan when they collect, process or use the personal data of Taiwan nationals.⁵³

10.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

The Financial Supervisory Commission is notably active in enforcing the regulations and guidelines it has established, alongside the provisions of the PDPA.

10.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

No. It is not lawful to purchase marketing lists from third parties.

10.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

The maximum penalty is NT\$200,000.⁵⁴

11 Cookies

11.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

There are no specific legislative restrictions on the use of

cookies. However, if cookies can be used to identify a natural person, whether directly or indirectly, especially in conjunction with other information, they may be regarded as personal data and thus subject to the provisions of the PDPA.

11.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

This is not applicable.

11.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

This is not applicable.

11.4 What are the maximum penalties for breaches of applicable cookie restrictions?

This is not applicable.

12 Restrictions on International Data Transfers

12.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Cross-border transfer of personal may be prohibited:

- 1. where major national interests are involved;
- 2. where an international treaty or agreement so stipulates;
- 3. where the country receiving the personal data lacks proper regulations on protection of personal data and the data subjects’ rights and interests may consequently be harmed; or
- 4. where the cross-border transfer of the personal data to a third country (territory) is carried out to circumvent the PDPA.⁵⁵

In these circumstances, the competent authority may impose restrictions on such transfer.

12.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract, with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

No further procedures/requirements are necessary for the transfer of personal data abroad, provided that such transfer is not restricted by the competent authority.

12.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

No, this is not required.

12.4 Do transfers of personal data to other jurisdictions require a transfer impact assessment? If conducting a transfer impact assessment is only mandatory in some circumstances, please identify those circumstances.

No, this is not required.

12.5 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?

No guidance has been issued.

12.6 What guidance (if any) has/have the data protection authority(ies) issued in relation to the use of standard contractual/model clauses as a mechanism for international data transfers?

No guidance has been issued.

13 Whistle-blower Hotlines

13.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

The PDPA does not mandate the establishment of a whistle-blower hotline, nor does it offer any exceptions regarding this matter. Thus, the collection, processing and use of personal data must adhere to general provisions in the PDPA.

13.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

This is not applicable.

14 CCTV

14.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

No, it does not.

14.2 Are there limits on the purposes for which CCTV data may be used?

If the CCTV data may be used to directly or indirectly identify a natural person, such data will be deemed as personal data and subject to the provisions of the PDPA. If so, the use of CCTV data must not exceed the necessary scope of specific purposes and must have legitimate and reasonable connections with the purposes of collection.⁵⁶ Nevertheless, if the usage falls under the statutory exceptions for using personal data for other purposes, such out-of-scope usage is permissible.⁵⁷

15 Employee Monitoring

15.1 What types of employee monitoring are permitted (if any), and in what circumstances?

In general, employee monitoring is permitted, provided that the collection, processing and use of personal data comply with the provisions of the PDPA.

15.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Not necessarily. Employers can argue that the employment contract provides them with the legal basis to monitor their employees.⁵⁸ Nonetheless, it is typical for such contracts to contain a consent clause, allowing employees to agree to or be informed about the collection, processing and use of their personal data for management purposes.

15.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

There is no requirement to notify or consult works councils/trade unions/employee representative.

15.4 Are employers entitled to process information on an employee's attendance in office (e.g., to monitor compliance with any internal return-to-office policies)?

Yes, they are.

16 Data Security and Data Breach

16.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Yes. Non-government agencies (i.e., companies) in possession of personal data files must implement proper security measures to prevent the personal data from being stolen, altered, damaged, destroyed or disclosed.⁵⁹ (There is no distinction between the data controllers, processors, etc. under the PDPA.)

16.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Yes, for some entities. For certain industries that have active regulations for the security and maintenance of personal information files in place, it is usually required to report material data breaches to the competent authority within 72 hours with details including the time of the incident, the type of breach, the underlying cause, a summary of the incident, the extent of the damage, potential outcomes of the data infringement, the countermeasures to be implemented, the timing and method of communication to those affected, etc.

16.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Yes, but the PDPA only stipulates that “the data subject shall be notified via appropriate means after the relevant facts have been clarified”.⁶⁰

16.4 What are the maximum penalties for personal data security breaches?

NT\$2 million for the first violation and NT\$15 million for a serious violation or if the company fails to rectify the previous violation in time.

17 Enforcement and Sanctions

17.1 Describe the enforcement powers of the data protection authority(ies).

- (a) **Investigative powers:** Initiate investigation, inspection and/or confiscate evidence on potential violation of the PDPA.⁶¹
- (b) **Corrective powers:** Order the company to rectify the violation within a specified period of time,⁶² prohibit the collection, processing or use of the personal data, order the erasure of the processed personal data and personal data files, confiscate or order the destruction of the unlawfully collected personal data and/or disclose to the public the violation of the non-government agency, the name of the non-government agency and its responsible person/representative.⁶³
- (c) **Authorisation and advisory powers:** Issue interpretation documents from when an inquiry is received.
- (d) **Imposition of administrative fines for infringements of specified legal provisions:** Impose a fine for each occurrence of the violation.⁶⁴
- (e) **Non-compliance with a data protection authority:** Please refer to (b) and (d) above.

17.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

No, it does not.

17.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

The data protection authority will carry out administrative inspections of companies, and if any instances of non-compliance are identified, the authority will initially issue a corrective order before imposing fines, if deemed necessary.

17.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

No, it does not.

18 E-discovery/Disclosure to Foreign Law Enforcement Agencies

18.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Typically, businesses do not take proactive measures in response to foreign e-discovery requests or requests from foreign law enforcement agencies unless they have an operational presence in that foreign jurisdiction. Under the PDPA, foreign law enforcement agencies are classified as non-governmental agencies, meaning their authority is not acknowledged within the framework of Taiwan’s PDPA. Consequently, businesses are not legally obligated to comply with such requests unless they are validated by a court or a government agency in Taiwan.

18.2 What guidance has/have the data protection authority(ies) issued on disclosure of personal data to foreign law enforcement or governmental bodies?

No guidance has been issued.

19 Artificial Intelligence

19.1 Are there any limitations on automated decision-making involving the processing of personal data using artificial intelligence?

No, there are not.

19.2 What guidance (if any) has/have the data protection authority(ies) issued in relation to the processing of personal data in connection with artificial intelligence?

The data protection authority has not issued any guidance in relation to the processing of personal data in connection with artificial intelligence.⁶⁵

20 Trends and Developments

20.1 In your opinion, what enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.

The competent authority has been actively inspecting whether the company has established a security and maintenance plan for the protection of personal data files or rules on disposing of personal data following a business termination, in accordance with Article 27 of the PDPA and regulations established by the authority.

Additionally, in the name of anti-fraud, recent amendments on the Communication Security and Surveillance Act

have granted the prosecutors and the judicial police officers to obtain the communications user information, if there are sufficient facts to determine that it is necessary and relevant to the investigation of the case.⁶⁶

20.2 In your opinion, what “hot topics” are currently a focus for the data protection regulator?

The Executive Yuan has prepared a draft amendment to the PDPA along with a proposed new regulation for the organisation of the Personal Data Protection Commission. This initiative aims to clearly define the duties and responsibilities of the consolidated authority.

Endnotes

- 1 Article 27 of the PDPA:
(Paragraph 2) The central government authorities in charge of the industries concerned may designate and order certain non-government agencies to establish a security and maintenance plan for the protection of personal data files and rules on disposing personal data following a business termination.
(Paragraph 3) Matters such as standards on setting forth the aforementioned plans and disposal regulations shall be expressly established by the central government authority in charge of the industry concerned.
- 2 Article 1-1, Paragraph 1 of the PDPA.
- 3 Article 2, Subparagraph 1 of the PDPA.
- 4 Article 2, Subparagraph 4 of the PDPA.
- 5 Article 7 of the Enforcement Rules of the PDPA.
- 6 Article 2, Subparagraph 9 of the PDPA.
- 7 Article 6 of the PDPA.
- 8 Article 2 of the Enforcement Rules of the PDPA.
- 9 Article 3 of the Enforcement Rules of the PDPA.
- 10 Article 2, Subparagraph 2 of the PDPA.
- 11 Article 5 of the Enforcement Rules of the PDPA.
- 12 Article 2, Subparagraph 3 of the PDPA.
- 13 Article 2, Subparagraph 5 of the PDPA.
- 14 Article 6, Paragraph 1 of the Enforcement Rules of the PDPA.
- 15 Article 6, Paragraph 2 of the Enforcement Rules of the PDPA.
- 16 Article 4, Paragraph 1 of the Enforcement Rules of the PDPA.
- 17 Article 4, Paragraph 2 of the Enforcement Rules of the PDPA.
- 18 Article 4, Paragraph 3 of the Enforcement Rules of the PDPA.
- 19 Article 4, Paragraph 4 of the Enforcement Rules of the PDPA.
- 20 Article 4, Paragraph 5 of the Enforcement Rules of the PDPA.
- 21 Article 4, Paragraph 6 of the Enforcement Rules of the PDPA.
- 22 Article 51, Paragraph 2 of the PDPA.
- 23 Article 51, Paragraph 1 of the PDPA.
- 24 Article 7, Paragraph 1 of the PDPA.
- 25 Article 7, Paragraph 2 of the PDPA.
- 26 Article 12 of the PDPA.
- 27 Article 19, Paragraph 1 of the PDPA.
- 28 Article 19, Paragraph 1 of the PDPA.
- 29 Article 5 of the PDPA.
- 30 Article 5 of the PDPA.
- 31 Article 3, Subparagraph 3 of the PDPA.
- 32 Article 5 of the PDPA.
- 33 Article 3, Subparagraph 1 of the PDPA.
- 34 Article 3, Subparagraph 3 of the PDPA.
- 35 Article 3, Subparagraph 5 of the PDPA.
- 36 Article 3, Subparagraph 4 of the PDPA.
- 37 Taiwan Constitutional Court Judgment 111-Hsien-Pan-13 (2022).
- 38 Article 10 of the PDPA.
- 39 MOJ Interpretation Document No. 10603512680.
- 40 Article 20, Paragraph 2 of the PDPA.
- 41 Article 20, Paragraph 3 of the PDPA.
- 42 Article 29, Paragraph 1 of the PDPA.
- 43 Article 32 of the PDPA.
- 44 Article 69, Paragraph 3 of the Protection of Children and Youths Welfare and Rights Act.
- 45 National Development Council Interpretation Document Fa-Fa No. 1100005839, National Development Council Interpretation Document Fa-Fa No. 1082000384, and MOJ Interpretation Document No. 10703503140.
- 46 Article 4, Paragraph 1 of the Human Biobank Management Act.
- 47 Article 2 of the Administrative Regulations on the Establishment of Human Biobank.
- 48 Article 3 of the Administrative Regulations on the Establishment of Human Biobank.
- 49 Article 23, Paragraph 1 of the Human Biobank Management Act.
- 50 Article 8 of the Administrative Regulations on the Establishment of Human Biobank.
- 51 <https://dep.mohw.gov.tw/DOMA/cp-3133-12824-106.html>
- 52 Article 12, Paragraph 2, Subparagraph 1 of the Enforcement Rules of the PDPA.
- 53 Article 51, Paragraph 2 of the PDPA.
- 54 Article 48, Paragraph 1, Subparagraph 3 of the PDPA.
- 55 Article 21 of the PDPA.
- 56 Article 5 of the PDPA.
- 57 Article 20, Paragraph 1 of the PDPA.
- 58 Article 19, Paragraph 1, Subparagraph 2 of the PDPA.
- 59 Article 27, Paragraph 1 of the PDPA.
- 60 Article 12 of the PDPA.
- 61 Article 22 of the PDPA.
- 62 Article 47 and 48 of the PDPA.
- 63 Article 25, Paragraph 1 of the PDPA.
- 64 Article 25, 47, 48, 49, and 50 of the PDPA.
- 65 <https://www.pdpc.gov.tw/CP/130>
- 66 Article 11-1 of the Communication Security and Surveillance Act.



Yvonne Y.F. Lin is the director and managing partner at Formosan Brothers. She is also an arbitrator and mediator registered with the Chinese Arbitration Association, Taipei, and a patent agent in Taiwan.

As a litigator, she has obtained extensive experience in leading and handling multi-jurisdictional dispute and litigation over the years and decades. Ms. Lin assists international telecom companies, pharmaceutical/medical device companies, semiconductor companies and clients from various industries for both litigious and non-litigious matters on data protection, intellectual property, licensing, anti-trust laws and general corporate laws. She represents leading international companies from the semiconductor industry, pharmaceutical/medical device industry, green energy industry and automobile industry on high-profile cases and provides comprehensive legal service to the clients.

Formosan Brothers Attorneys-at-Law
16F-6, No. 376, Sec. 4, Ren-Ai Rd.
Da'an, Taipei, 106434
Taiwan

Tel: +886 2 2705 8086 ext. 610
Email: yvonne@mail.fblaw.com.tw
URL: www.fblaw.com.tw/people-en/yvonne-y-f-lin



Jeffrey K.S. Hung graduated from the Public Law Division of the Graduate School of Law at National Taiwan University, with a thesis that focused on administrative litigation. In addition to practising law, he is also a Certified Privacy Management Professional (CPMP).

During his practice, Mr. Hung has provided advice to international and domestic companies from different industries for data protection and compliance matters over the years. Mr. Hung also participated in the defence of white-collar criminal cases involving the Anti-Corruption Act, the Securities and Exchange Act, the Insurance Act, and the Securities Investment Trust and Consulting Act. He has also handled commercial arbitrations related to shipbuilding and maritime incidents, as well as investigations and administrative litigation involving concerted actions. Lately, he has engaged in legal advisory work and dispute resolution for clients in the fields of offshore wind power and solar photovoltaic development, providing consultation and legal opinions on various energy-related matters.

Formosan Brothers Attorneys-at-Law
16F-6, No. 376, Sec. 4, Ren-Ai Rd.
Da'an, Taipei, 106434
Taiwan

Tel: +886 2 2705 8086 ext. 512
Email: kuohsun@mail.fblaw.com.tw
URL: www.fblaw.com.tw/people-en/jeffrey-k-s-hung



Jackie Yang has a cross-disciplinary professional background. In addition to her legal expertise, she also has a background in mechanical engineering and information technology, enabling her to provide comprehensive legal services to her clients.

After graduating from the Department of Mechanical Engineering at National Taiwan University, Ms. Yang pursued a Master's degree in mechanical engineering at Carnegie Mellon University in the United States. After graduation, she worked as an engineer at Coretech System, Trend Micro, and Garmin, accumulating extensive practical experience. She also obtained a Master's degree in Interdisciplinary Legal Studies from National Taiwan University with a thesis related to anti-money laundering.

As technology continues to evolve, new legal issues have emerged in areas such as labour law, data protection and the AI era. Ms. Yang's unique background gives her a distinct advantage in the legal field. Whether it is litigation cases, contract review, legal consultation or research on emerging issues, she can provide forward-looking and practical recommendations tailored to industry needs, and strives to achieve the best interests for her clients.

Formosan Brothers Attorneys-at-Law
16F-6, No. 376, Sec. 4, Ren-Ai Rd.
Da'an, Taipei, 106434
Taiwan

Tel: +886 2 2705 8086 ext. 522
Email: jackie@mail.fblaw.com.tw
URL: www.fblaw.com.tw/people-en/jackie-yang

Formosan Brothers was founded in 1997 and currently stands as one of Taiwan's preeminent full-service law firms. Over the past 28 years, through dedication and professionalism, Formosan Brothers established a foundation built atop our impeccable reputation.

Formosan Brothers boasts a team of legal professionals whose knowledge, experience and acumen are second to none. We offer an abundance of experience and a storied track record of success in data protection, medical technology and healthcare, intellectual property, construction, employment, banking, finance, etc. Many of our attorneys are licensed to practise both in Taiwan and foreign jurisdictions, contributing to our deep knowledge of international legal matters. Further, Formosan Brothers understands Taiwan's cultural and business nuances. Our international clients take comfort in knowing that we will combine

both international knowledge and domestic understanding to craft the most suitable solutions to transnational matters. This unique offering remains one of Formosan Brother's most acclaimed advantages.

www.fblaw.com.tw



Ukraine



Vladyslav Podolyak



Tetiana Partsei

Arriba

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

In Ukraine, the primary data protection law is the Law No. 2297-VI¹ “On Personal Data Protection” (“the Law”). Ukraine is also a party to Convention No. 108 (“108 Convention”)² and its Additional Protocol on supervisory authorities and cross-border data flows.

The Ukrainian Parliament Commissioner for Human Rights (also the “Data Protection Authority”, “DPA” or “Ombudsman”) oversees personal data protection and has issued omnibus bylaws that specify model procedures for processing data, supervisory controls and risk-based notifications, as follows: (i) the Model Procedure for the Processing of Personal Data; (ii) the Procedure for the Commissioner’s Oversight of Compliance with Personal Data Protection Legislation; and (iii) the Procedure for Notifying the Commissioner about: the processing of personal data that poses particular risks to the rights and freedoms of individuals; and the designated structural unit or responsible person in charge of organising data protection activities during processing.³

The DPA has approved the Order of Processing the Materials on Administrative Offences,⁴ which specifies how administrative offences on privacy in compliance are documented before they are sent for court trial.

The DPA also provides advisory guidance on topics such as consent, remote transactions, data protection in wartime and AI-related privacy concerns.⁵

The draft Bill No. 8153⁶ “On Personal Data Protection” (“the Bill”), registered in Parliament on 25 October 2022, has been adopted in the first reading, for further updates in the second and third readings. The Bill aligns Ukrainian terminology and principles with the EU GDPR.

For the avoidance of doubt, Ukraine is not a Member State of the EU and, therefore, is not directly subject to the GDPR.

1.2 Is there any other general legislation that impacts data protection?

The Civil Code of Ukraine⁷ guarantees personal non-property rights, including privacy and data protection. Related laws, such as the Law “On Information”⁸ and the Law “On Protection of Information in Information and Communication Systems”⁹ regulate information handling and security. The Administrative Offense Code¹⁰ and Criminal Code¹¹ provide penalties for privacy violations.

1.3 Is there any sector-specific legislation that impacts data protection?

The Law “On Electronic Identification and Electronic Trust Services”¹² requires trusted service providers to notify authorities and users of confidentiality or integrity breaches.

The Law “On the Fundamentals of the Legislation of Ukraine on Healthcare”¹³ regulates the creation, sharing and publication of medical information.

The Law “On Banks and Banking”¹⁴ and the Law “On Financial Services and Financial Companies”¹⁵ have additional privacy-related norms for the banking and finance sector.

1.4 What authority(ies) are responsible for data protection?

The Ukrainian Parliament Commissioner for Human Rights is the DPA, empowered to handle complaints, conduct inspections, access information and issue binding orders. General jurisdiction courts handle civil, administrative and criminal cases, including data protection violations. Upon receiving an offence report from the DPA, courts can impose fines and may order corrective actions such as stopping unlawful processing or deleting improperly collected data.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

The Law provides explicit definitions for certain terms; however, some concepts found in the GDPR lack equivalent or closely aligned definitions within the Law, as the Law primarily mirrors the principles of the 108 Convention, which predates the GDPR and uses different terminologies and frameworks.

- **“Personal Data”** means the information or a set of information about an identified or specifically identifiable individual. The Bill defines Personal Data as any information relating to an identified or identifiable individual.
- **“Processing”** means any action or set of actions, such as collection, recording, accumulation, storage, adaptation, modification, renewal, use and dissemination (dissemination, sale, transfer), depersonalisation and destruction of personal data, including using information (automated) systems. The Bill defines Processing as any operation or set of operations that is performed on personal data, whether or not by automated means,

such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, consultation, pseudonymisation, profiling, anonymisation, use, disclosure by transmission or dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

- **“Controller”**, or the specific term used in the Law is a “personal data owner”, means a natural or legal person who determines the purpose of processing personal data, establishes the composition of these data and the procedures for their processing, unless otherwise specified by law. The Bill defines Controller as any natural or legal person, public authority or any other body that, alone or jointly with others, determines the purposes and means of the processing of personal data, as well as other natural or legal persons for whom the purposes and means of the processing are determined by law.
- **“Processor”**, or the specific term used in the Law is a “personal data manager”, means a natural or legal person who is granted by the personal data owner or by law to process these data on behalf of the personal data owner. The Bill uses the term “operator”, which is identified as a natural or legal person who is granted by the personal data owner or by law to process these data on behalf of the controller.
- **“Data Subject”** (hereafter also **“Individual”**) means a natural person whose personal data are processed. Under the Bill, this definition will not be modified.
- **“Sensitive Personal Data”/“Special Categories of Personal Data”**, under Article 7 of the Law, is defined as “special categories of data”, which includes: racial and ethnic origin; political, religious or ideological beliefs; membership in political parties and trade unions; health status; sexual life; biometric data; genetic data; and data on criminal conviction. Under the Bill, these categories will also have special regulatory conditions. Please also see the broader definition of “risky data” below.
- **“Risky Data”** encompasses: (i) “sensitive data” (see above); and (ii) other risky data, such as: national origin; membership in religious organisations or ideologically oriented public associations; health being subject to administrative or criminal conviction; measures applied to the individual within the framework of pre-trial investigation; measures taken against the individual as provided by the Law “On Operative and Investigative Activities”; acts of violence committed against the individual; and the location and/or movements of the individual.
- **“Data Breach”** is not clearly defined in the Data Protection Law. Article 1 of the Law “On Protection of Information in Information and Communication Systems” defines a data breach (information leak) as the result of actions or inaction that lead to information processed in a system or by an information processing device becoming known or accessible to individuals and/or legal entities who are not authorised to access it.
The Bill defines data breach as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of personal data or access to personal data resulting from a violation of the requirements and conditions for the security of personal data processing.
- **“Third Party”** means any person, except for the individual, the personal data controller or processor, and the DPA, to whom personal data is transferred by the controller or processor of personal data.

- **“Depersonalisation of Personal Data”** means the removal of information that enables a person to be identified directly or indirectly.
- **“Consent of the Individual”** means the voluntary expression of will by a natural person (provided that they are informed) to grant permission for the processing of their personal data in accordance with the stated purpose of such processing, expressed either in written form or in a manner that allows for the conclusion that consent has been given. In the field of e-commerce, the consent of the individual may be granted during registration in the information and communication system of an e-commerce entity by placing a checkmark or other confirmation indicating permission for the processing of their personal data in line with the stated purpose, provided that such a system does not enable the processing of personal data prior to the placement of such confirmation.

3 Territorial and Material Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The Law applies to any entity (individual, public or private entity, resident or non-resident) that processes personal data in Ukraine.

The Bill will launch a special mechanism for non-resident data controllers/processors: they shall appoint a local representative and also cooperate with the DPA in Ukraine.

3.2 Do the data protection laws in your jurisdiction carve out certain processing activities from their material scope?

The provisions of the Law do not apply to the processing of personal data when such processing is carried out:

- (1) by an individual solely for personal or household purposes; or
- (2) exclusively for journalistic or creative activities, provided that a balance is maintained between the right to privacy and the right to freedom of expression.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
Pursuant to Article 6 (1) of the Law, the processing of personal data is carried out openly and transparently, using means and in a manner that is appropriate for the specified purposes of such processing.
Article 4 of the Bill specifies the principle of lawfulness, good faith and transparency similar to Article 5 of GDPR: personal data must be processed on the grounds provided for in the Bill. Personal data must be processed in a manner that provides for the individual to be duly informed about the processing of their personal data (collection, use and other processing, its method and scope), except in cases provided for in the Bill, in order to ensure the elimination of unforeseen processing for the individual.

■ **Lawful basis for processing**

Article 11 of the Law specifies six grounds for the processing of personal data:

- (1) the individual's consent;
- (2) under a law that allows data processing by a controller solely for the purpose of exercising the controller's authority;
- (3) the conclusion and execution of a contract to which the individual is a party or that is concluded in favour of the individual or for the implementation of measures preceding the conclusion of a contract at the request of the individual;
- (4) the protection of vital interests of the individual;
- (5) the necessity to fulfil the obligation of the controller provided for by law; or
- (6) the need to protect the legitimate interests of the controller or a third party to whom personal data is transferred, unless the need to protect the fundamental rights and freedoms of the individual in connection with the processing of their data outweighs such interests.

The Bill sets out practically the same principle and mirrors Article 6 of the GDPR.

■ **Purpose limitation**

Under Article 6 (1) of the Law, the purpose of data processing shall be specified in laws, other regulatory legal acts, regulations, corporate or other documents regulating the activities of the controller and comply with the privacy legislation.

The processing of personal data shall be carried out openly and transparently using means and in a manner that is appropriate for the specified purposes of such processing. If the specified purpose of data processing is changed to a new purpose that is incompatible with the previous one, in order to continue processing the data, the personal data controller must obtain the consent of the individual to process their data in accordance with the changed purpose unless otherwise provided by the Law.

Article 4 of the Bill sets out that data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes and mirrors Article 5 of the GDPR.

■ **Data minimisation**

The composition and content of personal data must be relevant, adequate and not excessive in relation to the purpose of their processing under Article 6(3) of the Law. The Bill reflects this principle in the same way and corresponds with the GDPR.

■ **Proportionality**

This principle is not established in the Law. The Bill refers to proportionality and proportional measures but does not explicitly reveal them.

■ **Retention**

Article 6(8) of the Law reads that the personal data shall be processed no longer than is necessary for the lawful purposes for which it was collected or further processed. Further processing of personal data for historical, statistical or scientific purposes may be performed provided they are adequately protected. Pursuant to Article 15 of the Law, personal data shall be deleted in the event of: (1) the expiration of the retention period determined by the individual's consent or by law; (2) termination of the legal relationship between the individual and the controller or processor, unless otherwise provided by law; (3) issuance of a relevant order by the DPA; or (4) entry into force of a court decision on the deletion or destruction of personal data.

Article 4 of the Bill reads that data must be kept in a form that permits identification of individuals for no longer than is necessary for the purposes for which the personal data are processed. This mirrors the GDPR storage limitation principle.

■ **Accuracy**

Per Article 6(2) of the Law, personal data must be accurate, reliable and updated as necessary for the purpose of its processing. The Bill elaborates: if it is found that personal data are inaccurate in relation to the purpose of their processing, such personal data must be rectified or deleted without undue delay.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

■ **Right of access to (copies of) data/information about processing**

Article 8(2) of the Law outlines the rights of individuals, including the right to know the sources, location and purpose of processing of their personal data, as well as the location of the controller or processor. Individuals also have the right to receive information about access conditions, access their personal data and obtain a response within 30 calendar days confirming whether their data is being processed and to receive the content of such data.

Article 19 of the Bill further grants individuals the right to receive, once free of charge, confirmation from the controller regarding the processing of their personal data. If processing occurs, they have the right to access the data and receive detailed information about processing purposes, categories of data, recipients, storage periods or criteria, their rights (including rectification, erasure, objection or restriction), the right to file a complaint, the source of data (if not collected directly), the existence of automated decision-making (including profiling) with an explanation of its logic and consequences, and safeguards for international transfers. All information must be presented clearly and be understandable. Access may be restricted only where necessary and proportionate to a legitimate aim.

The right to access may be restricted in the specific circumstances if such a restriction pursues a legitimate aim and is proportionate.

■ **Right to rectification of errors**

Article 20 of the Law reads that controllers and processors are obliged to rectify personal data per reasoned written request of the individual. Controllers and processors of personal data are obliged to rectify personal data also upon request of other eligible subjects, if there is the individual's consent or the relevant rectification shall be performed per instruction of the DPA or court. Inaccurate personal data shall be corrected without delay upon discovery of the error.

Under Article 20 of the Bill, individuals have the right to have inaccurate personal data corrected by the controller without undue delay, and no later than 30 days from the request. Individuals may provide or be asked to provide additional data for this purpose. Upon request, the controller must mark the data as disputed until a decision is made or, if appealed, until a final court ruling. The controller must also inform all data recipients of the correction, unless this would impose an undue burden.

■ **Right to deletion/right to be forgotten**

Per Article 8(2) the Law the individual has the right to submit a reasoned request for the modification or erasure of their personal data by any controller and processor of personal data if these data are processed unlawfully or are inaccurate. The right to be forgotten is not defined in the Law.

Under Article 21 of the Bill, the individual has the right to be forgotten – that is, to have their personal data erased by the controller without undue delay, and no later than 30 days from the request. This applies when: (i) the data is no longer needed for its original purpose; (ii) consent is withdrawn with no other legal basis for processing; (iii) the individual objects to processing and no overriding interest exists; (iv) the processing was unlawful; (v) the data was collected for information society services; or (vi) erasure is required by law. If the data was previously shared, the controller must take reasonable steps to inform other controllers to erase it as well.

■ **Right to object to processing**

Article 8(2) of the Law avails an individual to submit a reasoned request to the controller objecting to the processing of their data.

Article 22 of the Bill defines this right and states that the individual has the right to object at any time to the processing of their personal data based on public interest or legitimate interest, including direct marketing and profiling. The controller is obliged to stop further processing unless the processing of personal data is carried out on legal grounds that override the interests, rights and freedoms of the individual, or the processing is necessary for the submission, support or defence of a legal claim. The controller has a burden of proof as to the legal grounds for processing personal data. The controller must inform the individual about their rights no later than the first communication with them.

■ **Right to restrict processing**

Article 8(2) of the Law empowers individuals to make reservations regarding the restriction of the right to process their personal data when providing consent. The Bill clearly defines the right to restrict processing as follows: an individual may request restriction if (1) the accuracy of the data is contested – during the period of verification by the controller, (2) processing is unlawful, but the individual opts for restriction instead of erasure, (3) the controller no longer needs the data, but it is required by the individual for legal claims, or (4) the individual has objected to processing, pending a decision on whether the controller’s legitimate grounds override the individual’s rights and interests.

■ **Right to data portability**

The Law does not specifically include a right to data portability.

Under Article 23(1) of the Bill, the individual shall have the right to obtain from the controller a copy of any personal data concerning him or her collected by the controller during automated processing in a structured and machine-readable format, provided that the processing is carried out on a lawful basis. This right may be limited by law, provided the limitation serves a legitimate purpose and is necessary in a democratic society.

■ **Right to withdraw consent**

Article 8(2) of the Law ensures individuals’ right to withdraw consent to the processing of personal data. The Bill has more details: if the processing of personal data is based on the individual’s consent, they shall have

the right to withdraw consent at any time in the same manner as the consent was given (Article 6(8)).

■ **Right to object to marketing**

The Law does not contain specific provisions regarding direct marketing. Article 10(2) and 10(3) of the Law “On Electronic Commerce” reads that commercial electronic communications may be sent only if the recipient has given their consent to receive them. Such communications can be sent without prior consent only if the recipient has an opt-out option.

Article 12(3) of the Bill explicitly provides individuals with the right to withdraw their consent to processing for direct marketing purposes and the right to object to processing, including profiling for direct marketing, at any time.

■ **Right protecting against solely automated decision-making and profiling**

The Law gives individuals the right to protection from automated decision-making with legal effects (Article 8(2)). The Bill allows personal data processing for direct marketing – such as through social media, calls or emails – only with the individual’s explicit consent. Without consent, such processing is permitted only if: it follows a transaction involving the individual; it relates to similar products or services; the individual was informed and could opt out; and opting out is easy and without negative consequences. The individual may withdraw consent or object to processing, including profiling, at any time, and the controller must stop processing immediately upon request.

■ **Right to complain to the relevant data protection authority(ies)**

Article 8(2) of the Law empowers individual to submit complaints about the processing of their personal data to the DPA or to the court. The Bill contains the same provision relating to the right to complain (Article 26(1)).

■ **Right to compensation**

The Law does not explicitly establish a separate right to compensation. Therefore, individuals may refer to the general rules specified in Articles 16 and 22 of the Civil Code of Ukraine to seek compensation.

Under Article 26(2) of the Bill, an individual has the right to compensation for material and/or moral damage caused as a result of a violation of his/her rights. The controller shall be liable for the violation. The processor shall be liable for damage caused by processing only if the processor fails to comply with the obligations directly addressed to the processor, or if the processor acts contrary to the lawful instructions of the controller.

5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

Pursuant to the Law, individuals do not have an explicit right to mandate not-for-profit organisations to seek remedies on their behalf or to pursue collective redress. The Bill does not envisage collective redress either. The local legal system does not clearly endorse or accommodate the use of class action procedures. However, a remote mechanism for collective redress is available under the Consumer Protection Law. While not explicitly designed for data protection matters, it is possible that individuals may use more sophisticated approaches – such as membership-based schemes – to mandate a specific non-governmental organisation (whether

a consumer protection society or a privacy-focused NGO) to initiate a class action or legal proceedings on behalf of a defined group of individuals. While Supreme Court judges¹⁶ have clarified that legislation does not expressly prohibit class actions, we consider that a collective redress action specifically related to data protection would constitute a matter of first impression before the courts.

6 Children's Personal Data

6.1 What additional obligations apply to the processing of children's personal data?

The Law does not contain specific provisions regarding children (under 18). Therefore, we recommend obtaining consent for processing a child's personal data from a parent or legal guardian. Individuals aged 14 to 18 have limited legal capacity under Article 32 of the Civil Code of Ukraine, but it remains unclear whether this extends to giving valid consent for data processing. While the Law does not require age-appropriate language in consent forms or privacy policies, we advise ensuring clarity for individuals aged 14 to 18.

Articles 6 and 14 of the Bill introduce the following new rules: (i) individuals aged 14 and above may give consent themselves, while those under 14 require parental or guardian consent; and (ii) direct marketing and profiling for direct marketing purposes targeting children under 14 is prohibited.

7 Registration Formalities and Prior Approval

7.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

A notification rule applies only to processing "risky data". Pursuant to Article 9 of the Law, a controller who processes personal data which processing "constitutes a specific risk for rights and freedoms of individuals" must notify the DPA within 30 business days upon commencement of processing.

Notification rules are specified in the Order of the Parliamentary Ombudsperson¹⁷ dated 8 January 2014, No. 1/02-14. Exceptions apply to holding publicly available registers, NGOs and similar organisations that process their members' data and processing risky data by employers.

If passed into law, the Bill will cancel the above notification rule and will introduce the consulting rule instead (Articles 39 and 40). The Bill foresees that before initiating processing activities that are likely to pose a high risk to the rights and freedoms of natural persons, the controller must conduct a data protection impact assessment ("DPIA"). If the DPIA reveals that the intended processing would still result in a high risk – despite the mitigating measures and available costs/technologies – the controller is required to consult the DPA prior to proceeding.

7.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

The present notification rules imply that the controller must

complete a standard application form and lodge it with the DPA; the form has a rather general approach and must provide:

- Formal details about the data controller and data processor (*if any*): their full name, tax ID number, passport details and residence address of the individual, or company's name, registration number and company's address – for a legal entity.
- The general categories of "risky data" being processed.
- The purpose of the processing.
- The category or categories of individuals concerned.
- Third parties whom the personal data are shared with.
- Cross-border transfer details.
- The location (actual address) of the personal data processing.
- A general description of the technical and organisational measures implemented by the personal data controller to ensure data protection.

7.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

The processing of "risky data" triggers a mandatory notification procedure, meaning that if no risky data is processed, no notification is required. These notifications are organised by a legal entity; the other identifiers supplement searchability. The DPA periodically publishes lists of controllers that filed notifications. If a controller ceases to process "risky data", they shall serve a formal notice to the DPA within 10 working days upon cessation of data processing.

7.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

The answer departs from the scope of the Law, which, unlike the GDPR, has no extra-territorial scope. We conclude that resident controllers (individuals and local legal entities) are to follow the notification rule. There is no conclusive and compelling rule for non-residents that have no physical presence in Ukraine or run online processing of personal data of Ukrainian individuals. In practice, few representative offices of foreign legal entities performed the notification rules.

7.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

The notification form is a template document that includes both check-box options and fields requiring customised information to be completed by the data controller (see question 7.2).

7.6 What are the sanctions for failure to register/notify where required?

The penalty is applicable for failure to lodge a notification of processing "risky data" or for failure to lodge an updated notification. A penalty is imposed on:

- (1) the controller, if a natural person, ranging UAH 1,700–3,400 (approx. USD 40–80); repeated offence within a year is penalised UAH 5,100–8,500 (approx. USD 120–200);
- (2) the controller, if an individual entrepreneur, ranging UAH 3,400–6,800 (approx. USD 80–160); repeated offence within a year is penalised UAH 8,500–34,000 (approx. USD 200–800); or
- (3) the controller’s CEO, if a legal entity, ranging UAH 3,400–6,800 (approx. USD 80–160); repeated offence within a year is penalised UAH 8,500–34,000 (approx. USD 200–800).

7.7 What is the fee per registration/notification (if applicable)?

No fee is required for submitting a notification to the DPA.

7.8 How frequently must registrations/notifications be renewed (if applicable)?

The update form must be submitted within 10 working days if any previously filed information has changed. If the controller ceases to process “risky data”, they must provide notification to the DPA within 10 working days.

7.9 Is any prior approval required from the data protection regulator?

Under local law, data processing does not require prior approval. Article 40 of the Bill establishes a specific prior-consultation requirement that incorporates principles similar to those outlined in Article 36 of the GDPR.

7.10 Can the registration/notification be completed online?

Online filing of notification is available. A controller may download and complete the notification form, and then send the scanned document by email. Alternatively, the notification can be submitted by fax, regular mail or be delivered to a specially designated drop box at the office of the DPA. Online notification will be irrelevant if the Bill passes into law.

7.11 Is there a publicly available list of completed registrations/notifications?

The DPA periodically publishes lists of controllers that have filed notifications. Currently, such information can be found at the following link: <https://ombudsman.gov.ua/uk/zahist-personalni-danih>

If the Bill is adopted, the existing list of completed notifications will no longer hold legal relevance or practical applicability.

7.12 How long does a typical registration/notification process take?

From a practical perspective, the controller must submit the initial notification within 30 working days and updates within 10 working days. Once done, their obligation is fulfilled. The

DPA processes notifications in the order they are received, with no set timeframe. Controllers should monitor published lists of accepted and rejected notifications. If the Bill passes, notification requirements will no longer apply.

8 Appointment of a Data Protection Officer

8.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The appointment of a Data Protection Officer (“DPO”) is optional unless specific cases outlined in Article 24(2) of the Law apply, such as: (1) controllers/processors that process ‘risky data’; and (2) all state or municipal authorities. DPO functions may be carried out by an individual or a department. Article 41 of the Bill incorporates principles like those outlined in Articles 38 and 39 of the GDPR.

8.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

Failure to appoint a DPO does not, in itself, constitute a specific legal violation that would give rise to sanctions under current law. However, the absence of a DPO (if mandatory) may indicate a broader decline in overall privacy compliance.

Following the similar concept of administrative fines as provided in Article 83 of the GDPR, Article 59 of the Bill foresees a fine of (i) UAH 100,000–300,000 (approx. USD 2,380–7,140) if imposed on individuals, or (ii) UAH 300,000 (approx. USD 7,140) or 3–5% of a legal entity’s total annual turnover, whichever is higher, if imposed on legal entities.

8.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

The Law does not specify safeguards for the DPO role, so a DPO may be subject to general disciplinary or employment rules if they fail in their duties. In practice, a DPO’s status depends on the company’s culture, strategy and data protection priorities. Article 41 of the Bill ensures that a DPO cannot be dismissed, coerced into resignation, disciplined or subjected to adverse measures by the controller or processor for properly fulfilling their duties, mirroring Article 38(3) of the GDPR.

8.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

The Law does not provide a definitive position on this matter. We conclude that a DPO should be engaged as a part-time employee in each company where they fulfil the DPO role.

Article 41 of the Bill allows the appointment of a single DPO to cover multiple entities provided that the DPO is easily accessible from each entity, which mirrors the similar concept of Article 37 of the GDPR. A DPO may be a representative of a legal entity, an individual entrepreneur engaged in such activity under a contract, or an employee designated by the controller and/or processor.

8.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The Law does not set out specific requirements for the role, allowing considerable flexibility.

Article 41 of the Bill reads that a person may be appointed as a DPO if they hold a higher education degree of at least a bachelor's level and possess experience in the field of personal data protection. A person may not serve as a DPO if they: (i) have a criminal conviction for committing a serious or especially serious crime; (ii) have been declared partially incapacitated or incapacitated by a court decision; or (iii) have not passed the qualification examination – in the case of public authorities and controllers or processors engaged in large-scale processing of personal data.

8.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

Under Article 24 of the Law, the DPO is responsible for: (i) advising the controller or processor on privacy compliance; and (ii) engaging with the DPA to help prevent or address non-compliance. This allows controllers and processors considerable flexibility in how the role is implemented.

Article 41 of the Bill outlines more detailed DPO duties, aligning closely with Article 39(1) of the GDPR. These duties include: informing and advising the controller, processor and staff on data protection obligations; monitoring compliance, including assigning responsibilities and raising staff awareness; advising on and monitoring DPIAs; cooperating with the supervisory authority; acting as a contact point for the authority; and considering the risks related to personal data processing based on its nature, scope, context and purpose.

8.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

Per Article 24 of the Law, the controller or processor is required to notify the DPA of the appointment of a DPO by submitting a standard notification form within 30 working days of the DPO's appointment, and any subsequent updates must be reported within 10 working days.

Article 41 of the Bill reads that the controller or processor must publish the contact details of the DPO and communicate them to the DPA, which mirrors Article 37(7) of the GDPR.

8.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

The Law does not address this, allowing for broad flexibility.

Article 41 of the Bill requires the controller or processor to publish the DPO's contact details, but not necessarily in a public-facing privacy notice.

9 Appointment of Processors

9.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Article 3 of the Law has a minimum requirement that the controller must enter into an agreement with the processor in writing.

Article 31 of the Bill permits the engagement of a processor on the basis of either a contractual agreement or a legal act.

9.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

Article 4 of the Law reads that a controller–processor agreement must define the scope and purpose of data processing, allowing for broad flexibility. We recommend that the controller–processor agreement explicitly include the processor's obligations toward both the controller and individuals, establishing a minimum standard for privacy compliance and data security.

Article 31 of the Bill reads that the controller–processor agreement must define: the type and categories of personal data to be processed; the duration, nature and purpose of the processing; the type and categories of individuals concerned; and the rights and obligations of the controller, which obligations are rather broad and mirror similar rules specified in Article 28(3) of the GDPR.

10 Marketing

10.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

The Law has no specific rules on direct marketing, and processing someone's personal data for direct marketing may require general privacy compliance rules and case-by-case analysis. Article 14-3(2) of the Law of Ukraine "On Advertising" prohibits any form of spam (over five messages to one recipient) performed in electronic form or via phone calls without the consumer's prior written/electronic consent. Advertising using a person's phone number or other online contact details is only allowed if the person has given prior written/electronic consent. They must also be able to easily and clearly opt out at any time, free of charge, from having their data used or receiving such advertising. Furthermore, making bulk telephone, fax, electronic or other messages without the consumer's consent is aggressive business conduct that is prohibited by Article 19(5) of the Law of Ukraine "On Protection of Consumers' Rights".

Article 12 of the Bill specifies that personal data can only be used for direct marketing, political adverts or profiling if the person clearly agrees to it, unless certain legal exceptions apply. Without consent, marketing is only allowed if the data was collected during a contract, the marketing is for similar products, the person was told about it and could opt out easily at any time, and their privacy is not overly affected. Individuals can withdraw consent or object at any time, and the use of their data must stop immediately. If they object, their data must be deleted. Data of children under 14 years old cannot be used for marketing or marketing profiling at all.

10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

While these restrictions primarily target consumers and

individuals, the opt-in rule should be interpreted broadly, as it is also included in E-commerce law, which applies equally to both B2C and B2B commercial electronic messages sent to any recipient.

10.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

Making bulk telephone, fax, electronic or other messages without the consumer’s consent is aggressive business conduct that is prohibited by consumer protection law (see question 10.1). While there is no centralised opt-out register, individuals have the right to object to the processing of their personal data for direct marketing purposes at any time. Upon such objection, organisations are obligated to cease processing the individual’s data for marketing purposes immediately. This opt-out method might be used to cease unsolicited commercial communications by any means.

10.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?

The above restrictions as specified in Article 2(1) and 2(5) of the Law of Ukraine “On Advertising” apply to adverts if (i) they are not restricted for the Ukrainian audience by the advert publisher, or (ii) advertised goods are offered to persons located in Ukraine. By contrast, advertising law is not applicable to marketing activity that is performed by a legal entity that is located in the EU and when an advert is published in one of the EU official languages. However, the opt-out mechanism may be difficult to enforce, particularly against non-resident entities.

10.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

In general, the State Service of Ukraine on Food Safety and Consumer Protection is responsible for enforcing violations of marketing restrictions, while the National Bank of Ukraine supervises advertising in the banking and financial services sector. Individuals may also file complaints with the DPA in cases of privacy violations – this option will gain greater importance if the proposed Bill is passed into law.

10.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Buying a marketing list in Ukraine is legal if specific conditions under the Law are met. First, ensure that all individuals on the list have given informed, explicit consent for their data to be shared with third parties for marketing purposes, and that they were properly notified about such sharing. The buyer must have a valid legal basis for processing the data, typically consent, and must take steps to protect the data from unauthorised access or misuse. It is highly recommended to check with the seller whether any individuals on the list have previously opted out or unsubscribed from marketing communications, as this may constitute a withdrawal of consent and

make further use of their data unlawful. It is also essential to verify that the seller collected the data lawfully and fulfilled all legal requirements, including privacy notices and individuals’ rights. Buyers must be ready to honour opt-out requests and other individuals’ rights, such as access or deletion. All steps taken should be documented to ensure compliance. If the Bill is adopted, the core concept will remain, but with expanded details.

10.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Advertisers, producers and distributors who violate the Law “On Advertising” face a fine equal to five times the cost of the advertising or its production. If the violation is repeated within a year, the fine doubles. The advert cost is based on the advertising contract, and if the contract cost is not provided, the fine is UAH 1,700 (approx. USD 40).

11 Cookies

11.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

Ukraine has not implemented any specific legislation addressing the use of cookies, similar to the EU’s ePrivacy Directive. Not all websites have cookie settings and cookie consent mechanisms in place, unlike the majority of websites in the EU.

The Bill, if passed into law, will introduce specific rules that allow the use of cookies and similar tracking technologies if: (1) the individual has given explicit consent; (2) the processing is necessary for the operation of software, apps, websites or other electronic communication technologies; (3) the processing is strictly necessary to provide a service requested by the individual; or (4) the processing is needed to ensure data security, prevent fraud or protect against unauthorised interference with digital platforms or technologies.

11.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

At present, Ukrainian law does not explicitly regulate the use of cookies, neither distinguish different types of cookies. Some website operators in Ukraine voluntarily align their cookie consent mechanisms with EU standards, closely monitoring developments in EU best practices. Once the Bill is enacted, it will be possible to distinguish between strictly necessary cookies and those that require an individual’s consent or other lawful basis ground.

11.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

Due to the lack of underlying laws, the DPA has not carried out any enforcement actions or issued guidelines in this specific area. Once the Bill is enacted, the DPA will take a more proactive approach in identifying instances of privacy non-compliance related to the use of cookies and the enforcement of individuals’ privacy rights.

11.4 What are the maximum penalties for breaches of applicable cookie restrictions?

Currently, Ukrainian law does not impose any penalties for the misuse of cookies.

Under Article 59(1)(2) of the Bill, minor non-compliance with cookie regulations will incur fines ranging from 10,000 to 30,000 UAH (approx. USD 240 to 715) for individuals. For businesses, the penalty will be a turnover-based fine of 0.05% to 0.1%, with a minimum fine of 30,000 UAH (approx. USD 715). In cases where non-compliance results in a violation of privacy rights, individuals will face fines ranging from 30,000 to 100,000 UAH (approx. USD 715 to 2,380). For businesses, the penalty will be a turnover-based fine of 0.5% to 1%, with a minimum fine of 100,000 UAH (approx. USD 2,380).

12 Restrictions on International Data Transfers

12.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Under the Law, personal data may be transferred only if the receiving state ensures adequate protection as defined by Ukrainian law or international treaties. EEA Member States and 108 Convention signatories are recognised as providing adequate protection (Article 29(3)). The same applies to states whose capital market regulators have signed the IOSCO Multilateral Memorandum. On 16 August 2022, Ukraine's Government issued a list of such states.

Data may also be transferred with (i) clear consent of the individual, (ii) necessity for contract execution, (iii) protection of the individual's vital interests, (iv) public interest or legal requirements, or (v) guarantees from the data owner against interference with the individual's private life (Article 29(4)). However, data cannot be used for purposes other than those originally collected.

Under the Bill, transfers are allowed if (i) the foreign state or organisation ensures adequate protection, (ii) appropriate safeguards are in place, or (iii) approved binding corporate rules exist (Article 44).

12.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

Businesses often obtain explicit and informed individual's consent before transferring their personal data to a foreign country or international organisation. This is a key mechanism, especially when other legal grounds are not applicable. Personal data may be transferred abroad without the need for additional consent, provided the transfer is aligned with the terms of the contract.

Standard contractual clauses or other contractual mechanisms are not approved by regulatory authorities.

12.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection

authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

Registration or notification are not required by the Law.

12.4 Do transfers of personal data to other jurisdictions require a transfer impact assessment? If conducting a transfer impact assessment is only mandatory in some circumstances, please identify those circumstances.

The Law does not require a transfer impact assessment.

Article 48(4) of the Bill provides that a transfer impact assessment may serve as a non-recurrent ground for cross-border data transfer.

12.5 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?

The DPA has not issued any guidance on the *Schrems II* case.

12.6 What guidance (if any) has/have the data protection authority(ies) issued in relation to the use of standard contractual/model clauses as a mechanism for international data transfers?

The DPA has not issued any guidance on the use of standard contractual/model clauses.

13 Whistle-blower Hotlines

13.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

There is currently no whistleblowing legislation covering private companies or employees who report misconduct, so internal HR or customer service hotlines are not legally recognised as whistleblowing channels. However, under the Law "On Amendments to the Prevention of Corruption Law of Ukraine"¹⁸ (adopted on 1 June 2021, effective since 26 June 2021), a single national whistle-blower portal was established to report corruption. A whistle-blower is defined as someone who, believing the information to be credible, reports suspected corruption or related offences learned through their work, studies or legal involvement.

13.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Whistle-blower anonymity is protected only in the public sector and limited to corruption-related cases. Under the Law "On Citizen's Petitions",¹⁹ anonymous submissions are not required to be reviewed, which may discourage treating such reports as credible evidence or valid grounds for investigation.

Some global companies promote a culture of compliance by operating whistleblowing hotlines managed by their head office, which are also available to employees of their subsidiaries in Ukraine for HR and compliance-related matters.

14 CCTV

14.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

The current privacy legislation does not contain specific provisions regarding CCTV. The law does not require separate registration, notification or prior approval from the DPA for CCTV use, nor does it mandate any specific form of public notice. Pursuant to Article 307(1) of the Civil Code of Ukraine, a natural person may only be photographed, filmed or recorded on video with their consent. Consent is presumed if the recording occurs publicly, such as on the street, at gatherings, conferences, rallies or other public events.

Pursuant to Article 10 of the Bill, a specific CCTV notice will be required, containing the contact details of the controller, and a more restrictive approach will be introduced regarding CCTV use.

14.2 Are there limits on the purposes for which CCTV data may be used?

Article 307(1) of the Civil Code of Ukraine mandates non-hidden recording of public areas or events.

Article 10 of the Bill will pursue a purpose-limitation concept. Video surveillance by authorities is allowed in public spaces, including transport, only for crime prevention and public safety, as per the Law. Private individuals or entities may conduct surveillance to protect property within their own premises. Surveillance is only permissible if less intrusive methods cannot achieve the same goals. The regulator approves procedures, and operators must display a notice about the surveillance. Personal data collected cannot be used for other purposes, and surveillance in private areas is prohibited unless authorised by law. Data can be stored for up to six months. Surveillance is not allowed in areas where individuals expect privacy, and any recorded data must be properly stored with clear documentation of access. These rules also apply to photography and video recording for similar purposes.

15 Employee Monitoring

15.1 What types of employee monitoring are permitted (if any), and in what circumstances?

While local privacy law does not specifically address employee monitoring, the Labour Code establishes the employer’s right to oversee employees and maintain workplace discipline. This general provision may serve as a reasonable legal basis for implementing employee monitoring practices, particularly where such monitoring is proportionate and supported by available technologies.

Pursuant to Articles 51–55 of the Bill, employers in Ukraine may process employees’ personal data for employment-related purposes, such as hiring, managing, evaluating and terminating employment. This includes monitoring via information

and communication technologies, such as video surveillance (CCTV), automated systems and digital tracking tools. Any such processing must be lawful, proportionate and transparent. Employers must inform employees in advance about monitoring methods (including use of video or recordings at the workplace). Employees have the right to access and challenge evaluations or decisions based on their data. Automated decisions that significantly affect employees’ rights are prohibited without considering the employee’s viewpoint. Special rules apply to sensitive data like health or biometric data, which can only be collected in limited, justified cases. Employers must also implement safeguards and internal policies for handling employee data and provide these policies to staff.

15.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

The Labour Code²⁰ of Ukraine requires employers to inform employees about working conditions, including any monitoring systems like CCTV, before work begins. Under the Bill, employers must also inform employees about personal data processing through technologies such as video surveillance (Article 55(2)). Employees have the right to request details and justification for the processing of their personal data (Article 55(5)).

15.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

Neither the Law nor the Bill include any requirements to notify councils or trade unions.

15.4 Are employers entitled to process information on an employee’s attendance in office (e.g., to monitor compliance with any internal return-to-office policies)?

The Law and the Bill do not set specific prohibitions or restrictions on this matter. Since absenteeism is a form of misconduct that can lead to reprimand or dismissal, documenting misconduct is lawful, allowing employers to process attendance data. However, employee monitoring becomes more complex in the modern context, where remote work is common and may require more nuanced legal approaches.

16 Data Security and Data Breach

16.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Article 24(1) of the Law imposes a general obligation to ensure the security of personal data. Both controllers and processors are required to implement appropriate technical and organisational measures to protect personal data from unauthorised access, loss, destruction or unlawful processing.

Article 35(1) of the Bill mandates that the controller and processor must take suitable technical and organisational steps to ensure personal data is processed securely, with measures matching the level of risk to individuals’ rights and freedoms. Controller and processor may implement measures such as data encryption, regular testing of security measures, and ensuring the confidentiality, integrity and availability of data.

16.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

The Law does not require data breaches to be reported to the DPA. Pursuant to Article 9 of the Law “On Protection of Information in Information and Communication Systems”, only those who manage information and communication systems holding state information resources or classified data are required to report data breaches, which is not exactly the same as the data breach concept.

According to the Article 37 of the Bill, personal data controllers must notify the DPA of any data breach, unless it is unlikely to pose a risk to individuals’ rights and freedoms. This notification must be submitted without delay and no later than 72 hours after becoming aware of the breach. It should detail how the breach occurred, the number of affected individuals, the types and volume of compromised data, the contact details of the responsible person, the potential consequences, and any measures taken or planned to address the breach.

16.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Under the Law, data controllers are not legally required to inform affected individuals when a personal data breach occurs.

The Bill introduces a legal obligation for data controllers to notify affected individuals in the event of a data breach. This notification must include the same information that is required to be submitted to the DPA. The controller is not required to notify the individuals if: (1) strong security measures were in place that protected the data; (2) steps were taken to prevent serious risk to the individuals; and (3) notification would be an excessive burden.

16.4 What are the maximum penalties for personal data security breaches?

Administrative penalties under Article 188-39 of the Code of Administrative Offences range from a few hundred to several thousand UAH, with a maximum of UAH 34,000 (approx. USD 820) for repeat offences. Current laws offer only basic cybersecurity requirements, such as antivirus use and access control. Under Article 182 of the Criminal Code, unlawful handling of confidential information can lead to fines up to UAH 17,000 (approx. USD 410), corrective labour, or up to three years of restricted freedom, though criminal cases are rare. The Bill significantly raises penalties, allowing fines up to UAH 150 million (approx. USD 3.6 million) or 8% of a company’s annual turnover, and up to UAH 20 million (approx. USD 482,000) for individuals (Article 59).

17 Enforcement and Sanctions

17.1 Describe the enforcement powers of the data protection authority(ies).

- (a) **Investigative powers:** The DPA may carry out scheduled or unscheduled, on-site or remote inspections of controllers or processors, based on complaints or on its own initiative, with access to premises where personal data is processed, as permitted by law. Also, the DPA is empowered to demand explanations, documents or other materials related to personal data processing.
- (b) **Corrective powers:** The DPA may issue binding orders to address violations of data protection law, including: instructions to modify, delete or destroy personal data; ensure access to data; allow or restrict disclosure to third parties; or suspend or terminate data processing activities.
- (c) **Authorisation and advisory powers:** The DPA has the authority to: provide recommendations on the practical application of privacy laws to controllers, processors and individuals; receive proposals, complaints and other appeals from individuals and legal entities on issues of data protection; and make decisions based on the results of their consideration.
- (d) **Imposition of administrative fines for infringements of specified legal provisions:** Unlike under the GDPR, the DPA in Ukraine cannot independently impose fines for personal data protection violations. Instead, it prepares an administrative offence report, and only a court can hear the case and impose a fine.
- (e) **Non-compliance with a data protection authority:** The DPA has the authority to refer cases to court if a violation may constitute an administrative offence and involve liability under the Law.

17.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

Based on an inspection or application review, the DPA may issue binding instructions to prevent or correct violations of personal data law. These may include orders to: change, delete or destroy data; ensure access; allow or prohibit sharing with third parties; or suspend or stop processing. There is no necessity to require a court order to enforce binding instructions.

17.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

The DPA currently relies on a corrective and advisory approach to promote compliance with personal data laws, with limited enforcement of fines and no clear examples of strategic data protection enforcement. However, the adoption of the Bill is expected to grant the DPA stronger enforcement powers, potentially leading to more decisive action against future violations.

17.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

There is no straightforward enforcement mechanism for the DPA to exercise authority over businesses based outside of Ukraine. In the most serious cases, the DPA may rely on Mutual Legal Assistance Treaty mechanisms or seek court action for enforcement abroad.

18 E-discovery/Disclosure to Foreign Law Enforcement Agencies

18.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Ukrainian businesses typically attempt to avoid responding to foreign e-discovery requests or disclosure demands unless they are supported by a Ukrainian court decision or a treaty obligation between states.

18.2 What guidance has/have the data protection authority(ies) issued on disclosure of personal data to foreign law enforcement or governmental bodies?

There is no guidance from the DPA on this topic.

19 Artificial Intelligence

19.1 Are there any limitations on automated decision-making involving the processing of personal data using artificial intelligence?

The Law grants individuals the right to protect against solely automated decision-making (see question 5.1) but does not address other challenges posed by AI technologies.

The Bill extends this protection by giving individuals the right to be informed about automated decision-making, including profiling, and the algorithms used. It also defines profiling as a form of automated processing aimed at assessing individual characteristics, such as behaviour patterns, health status and preferences (Article 19). Additionally, the Bill requires controllers to assess the impact of large-scale automated data processing, including profiling, when it results in legal or similarly significant effects.

19.2 What guidance (if any) has/have the data protection authority(ies) issued in relation to the processing of personal data in connection with artificial intelligence?

The DPA did not issue any binding guidance regarding AI.

The DPA and Ministry of Digitalisation of Ukraine developed a methodological material “Human Rights in the Age of Artificial Intelligence: Challenges and Legal Regulation”, which examines the impact of the latest AI technologies on human rights and approaches to its legal regulation.²¹

20 Trends and Developments

20.1 In your opinion, what enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.

As the Bill is still pending its second reading in Parliament, enforcement remains based on the current law, which provides a simplified regulatory framework compared to EU standards. The DPA has issued Guidance²² on the protection of personal data during martial law, which was declared on 24 February 2022 and has been repeatedly extended through 2025. This guidance emphasises that certain restrictions on human rights during martial law may be justified for national security purposes. At the same time, safeguarding personal data against breaches resulting from cyberattacks and other hostile activities becomes even more critical under such conditions. Providing charity assistance to persons who suffered from war aggression normally implies consent.

The DPA conducts scheduled privacy compliance inspections across state authorities, municipalities and private sector entities (approx. 25–26 entities per quarter).

The DPA provides translations of EDPB guidelines, which may serve as a methodological foundation for future privacy trends in Ukraine.

Bill No. 6177,²³ dated 18 October 2021, which supports the idea of a separate DPA, has not gained any progress over the last year.

20.2 In your opinion, what “hot topics” are currently a focus for the data protection regulator?

The key focus areas remain consistent with last year, primarily centred on protecting privacy during wartime, particularly in the context of cyberattacks on critical infrastructure and data-driven services, as well as addressing new challenges from global digitalisation and AI. Notably, the DPA, which operates under the broader mandate of the Parliamentary Human Rights Commissioner, prioritises human rights more broadly, meaning wartime violations carry greater weight in its activities.

Endnotes

- 1 <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
- 2 https://zakon.rada.gov.ua/laws/show/994_326#Text
- 3 https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text
- 4 https://zakon.rada.gov.ua/laws/show/v3_02715-15#Text
- 5 <https://ombudsman.gov.ua/uk/rekomendaciyi-ta-rozysnennya>
- 6 <https://itd.rada.gov.ua/billInfo/Bills/Card/40707>
- 7 <https://zakon.rada.gov.ua/laws/show/435-15#Text>
- 8 <https://zakon.rada.gov.ua/laws/show/2657-12#Text>
- 9 <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>
- 10 <https://zakon.rada.gov.ua/laws/show/80731-10#Text>
- 11 <https://zakon.rada.gov.ua/laws/show/2341-14#Text>
- 12 <https://zakon.rada.gov.ua/laws/show/2155-19#Text>
- 13 <https://zakon.rada.gov.ua/laws/show/2801-12#Text>
- 14 <https://zakon.rada.gov.ua/laws/show/2121-14#Text>

- 15 <https://zakon.rada.gov.ua/laws/show/1953-20#Text>
- 16 <https://supreme.court.gov.ua/supreme/pres-centr/news/1376115>
- 17 https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text
- 18 <https://zakon.rada.gov.ua/laws/show/1700-18#Text>
- 19 <https://zakon.rada.gov.ua/laws/show/393/96-%D0%B2%D1%80#Text>
- 20 <https://zakon.rada.gov.ua/laws/show/322-08#Text>
- 21 https://ombudsman.gov.ua/storage/app/media/uploaded-files/%D0%9F%D0%A0%D0%90%D0%92%D0%90%20%D0%9B%D0%AE%D0%94%D0%98%D0%9D%D0%98%20%D0%92%20%D0%95%D0%9F%D0%9E%D0%A5%D0%A3%20%D0%A8%D0%A2%D0-A3%D0%A7%D0%9D%D0%9E%D0%93%D0%9E%20%D0%86%D0%9D%D0%A2%D0%95%D0%9B%D0%95%D0%9A%D0%A2%D0%A3_compressed.pdf
- 22 <https://ombudsman.gov.ua/storage/app/media/%D0%92%D0%BE%D1%94%D0%BD%D0%BD%D0%B8%D0%B9%20%D1%81%D1%82%D0%B0%D0%BD/%D0%97%D0%B0%D1%85%D0%B8%D1%81%D1%82%20%D0%BF%D0%B5%D1%80%D1%81%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D1%85%20%D0%B4%D0%B0%D0%BD%D0%B8%D1%85/%D0%97%D0%B0%D1%85%D0%B8%D1%81%D1%82%20%D0%BF%D0%B5%D1%80%D1%81%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D1%85%20%D0%B4%D0%B0%D0%BD%D0%B8%D1%85%20%D0%B2%20%D1%83%D0%BC%D0%BE%D0%B2%D0%B0%D1%85%20%D0%B2%D0%BE%D1%94%D0%BD%D0%BD%D0%BE%D0%B3%D0%BE%20%D1%81%D1%82%D0%B0%D0%BD%D1%83.pdf>
- 23 http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=72992



Vladyslav Podolyak is the Managing Partner at Arriba and has served as Co-Head of the Privacy and Cybersecurity practice since 2017. His focus extends beyond data privacy to include intellectual property, litigation and market entry support for businesses. From 2004 to 2017, he built a strong track record at PricewaterhouseCoopers and leading Ukrainian law firms. Mr. Podolyak advises data-driven businesses and has deep expertise in sectors such as social media, e-commerce, automotive and consumer goods. Mr. Podolyak is Of Counsel for the Ukrainian Parliament.

Arriba

Velyka Zhytomyrska Street, Building 8/14, Office 5
Kyiv, 01001
Ukraine

Tel: +380 67 352 52 99
Email: podolyak@arriba.legal
LinkedIn: www.linkedin.com/in/vladyslav-podolyak-35a12947



Tetiana Partsei is an Associate Lawyer at Arriba, where she has served as Co-Head of the Privacy and Cybersecurity practice since 2019. In her role, Tetiana advises clients on a wide range of matters related to data privacy, cybersecurity and regulatory compliance. Her expertise includes developing data protection strategies, ensuring alignment with both national and international privacy laws. Tetiana regularly supports companies by offering practical legal guidance tailored to the needs of businesses operating in the digital age. She holds her law degree from the National University of Kyiv-Mohyla Academy, where her academic focus culminated in a thesis on the legal regulation of facial recognition technology. Tetiana was admitted to the Ukrainian Bar and is an active participant in the evolving field of tech law.

Arriba

Velyka Zhytomyrska Street, Building 8/14, Office 5
Kyiv, 01001
Ukraine

Tel: +380 66 536 93 42
Email: maksymovych@arriba.legal
LinkedIn: www.linkedin.com/in/tetiana-maksymovych-17747820b

Arriba is a legal crew with an in-house lawyer’s mindset that protects critical business priorities safely and efficiently. We deliver legal advice for corporate clients across a wide range of industries, market sectors and geographies, *inter alia*: global companies producing power tools and consumer electronics, vehicles and automotive solutions, heavy industry, agrochemicals, FMCG, CPG, pharma; or that run global mobile apps and online global projects, create copyrighted content, e-commerce and international trade. These are our industry clients. Arriba collaborates in the best teams together with international law firms (Top 30 of the world rankings) that need a local legal advisor. Therefore, we synchronise our services to world-class standards. Arriba is always focused on cost/benefit and delivers safe, non-obvious and original legal solutions.

www.arriba.legal



United Arab Emirates



Saifullah Khan



Saeed Hasan Khan

Bizilance Legal Consultants

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

Federal Decree Law No. 45 of 2021 on personal data protection is the principal legislation applicable in the United Arab Emirates (UAE), except for the free zones, which have a specific law on personal data protection (the UAE Law).

The Dubai International Financial Centre (DIFC) Law No. 5 of 2020 (DIFC Law) is applicable over the DIFC. The DIFC is a free zone.

The Abu Dhabi Global Market (ADGM) Data Protection Regulations 2021 (ADGM Regulations) are applicable over the ADGM. The ADGM is also a free zone.

1.2 Is there any other general legislation that impacts data protection?

Federal Decree Law No. 34 of 2021 on Countering Rumours and Cybercrimes criminalises certain acts to be offences punishable with imprisonment and fine. Collecting and processing personal data and information in violation of the legislation is among one of the crimes that are subject matter of the referred law.

Federal Decree Law No. 33 of 2021, regarding the regulation of employment relationships, provides that workers shall keep the confidentiality of information and data to which they have access by virtue of their work.

1.3 Is there any sector-specific legislation that impacts data protection?

Sector-specific legislation governs data protection in their respective sectors, as follows:

- Federal Law No. 14 of 2018 (concerning the Central Bank of the UAE) governing data protection of customers of the banks.
- Federal Law No. 3 of 2003 (concerning telecommunication) governing data protection of telecom consumers.
- Federal Law No. 2 of 2019 (concerning use of information and communication technology in health fields) governing confidentiality of the patients' information.

1.4 What authority(ies) are responsible for data protection?

The UAE Data Office is the regulator for the purposes of the UAE Law.

- The Commissioner is to administer the DIFC Law.
- The Commissioner of Data Protection is responsible for the monitoring and enforcement of the ADGM Regulations.
- The Central Bank of the UAE and the Telecommunication and Digital Government Regulatory Authority (TDRA) are the regulators concerning the banking and telecommunication sectors, responsible for (among others) the protection of their respective consumers' data.

Health authorities (federal or local government) are entrusted for the protection of patients' data.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **"Personal Data"**
 - **The UAE Law:** Any data relating to an identified natural person, or a natural person who can be identified, directly or indirectly, through the linking of data, by reference to an identifier such as his or her name, voice, picture, identification number, electronic identifier, geographical location, or one or more physical, physiological, cultural or social characteristics. Personal data includes sensitive personal data and biometric data.
 - **The DIFC Law:** Any information referring to an identified or identifiable natural person.
 - **The ADGM Regulations:** Any information relating to a data subject.
- **"Processing"**
 - **The UAE Law:** An operation or set of operations which is performed on personal data using any electronic means including other means, such as collection, storage, recording, structuring, adaptation or alteration, handling, retrieval, exchange, sharing, use, characterisation, disclosure by transmission, dissemination, distribution or otherwise making available, alignment, combination, restriction, erasure, destruction or creation of a model of personal data.

- **The DIFC Law: Process, Processed, Processes and Processing (and other variants):** Any operation or set of operations performed upon personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage and archiving, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, transfer or otherwise making available, alignment or combination, restricting (meaning the marking of stored personal data with the aim of limiting processing of it in the future), erasure or destruction, but excluding operations or sets of operations performed on personal data by:
 - (a) a natural person in the course of a purely personal or household activity that has no connection to a commercial purpose; or
 - (b) law enforcement authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and preventing threats to public security.
- **The ADGM Regulations:** Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- **“Controller”**
 - **The UAE Law:** The establishment or the natural person who is in the possession of the personal data and who by virtue of its activity alone or jointly with others determines the means, methods, standards and purposes of the processing of personal data.
 - **The DIFC Law:** Any person who alone or jointly with others determines the purposes and means of the processing of personal data.
 - **The ADGM Regulations:** A natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- **“Processor”**
 - **The UAE Law:** An establishment or a natural person who processes the personal data on behalf of the controller and under his or her supervision and instructions.
 - **The DIFC Law:** Any person who processes personal data on behalf of a controller.
 - **The ADGM Regulations:** A natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller.
- **“Data Subject”**
 - **The UAE Law:** The natural person to whom personal data relates.
 - **The DIFC Law:** The identified or identifiable natural person to whom personal data relates.
 - **The ADGM Law:** An identified or identifiable living natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- **“Sensitive Personal Data”/“Special Categories of Personal Data”**
 - **The UAE Law:** Any information that directly or indirectly reveals a person’s race, ethnicity, political or philosophical views, religious beliefs, criminal record, biometric data, or any data related to such person’s health such as his or her physical, psychological, mental, corporal, genetic or sexual state, including any information related to such person’s provision with healthcare services that reveal his or her health condition.
 - **The DIFC Law: Special Categories of Personal Data:** Personal data revealing or concerning (directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal record, trade union membership and health or sex life and including genetic data and biometric data where it is used for the purpose of uniquely identifying a natural person.
 - **The ADGM Regulations: Special Categories of Personal Data:**
 - (a) personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs;
 - (b) genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation; and
 - (c) personal data relating to criminal convictions and offences or related security measures.
- **“Data Breach”**
 - **The UAE Law:** A breach of security and personal data through unauthorised or unlawful access thereto, such as replication, transmission, distribution, exchange, transfer, circulation or processing in such a manner leading to the disclosure or divulgence to third parties, or otherwise the destruction or modification of such data while being stored, transferred and processed.
 - **The DIFC Law/the ADGM Regulations: Personal Data Breach:** A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
- **“Consent”**
 - **The UAE Law:** The consent by which the data subject authorises third parties to process personal data relating to him or her, provided that such consent is a clear, specific and unambiguous indication of the data subject’s agreement by a statement or clear affirmative action, to the processing of the personal data relating to him or her.
 - **The DIFC Law:** Consent must be freely given by a clear affirmative act that shows an unambiguous indication of consent if it is to be relied on as a basis for processing. If the performance of an act by a controller, a data subject or any other party (including the performance of contractual obligations) is conditional on the provision of consent to process personal data, then such consent will not be considered to be freely given with respect to any processing that is not reasonably necessary for the performance of such act or where the consent relates to excessive categories of personal data. (The term “consent” is not defined. Conditions of consent are described at Section 12(1) of the DIFC Law.)

- **The ADGM Regulations:** Consent means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they (whether in writing, electronically or orally), by a statement or by a clear affirmative action, signify agreement to the processing of personal data relating to him or her.

3 Territorial and Material Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The UAE Law, the DIFC Law and the ADGM Regulations have extra territorial scope. In the following circumstances, a business established in another jurisdiction would be subject to these laws:

- **The UAE Law:** A controller or processor not established in the UAE that conducts personal data processing activities for data subjects who are in the UAE.
- **The DIFC Law:** The DIFC Law is applicable to a controller or processor regardless of its place of incorporation that processes personal data in the DIFC as part of stable arrangements.
- **The ADGM Regulations:** The ADGM Regulations are applicable when a processor is processing personal data for a controller outside the ADGM. In this case, the processor is to comply with the ADGM Regulations to the extent possible, taking into account whether the controller is subject to similar obligations under its home jurisdiction.

3.2 Do the data protection laws in your jurisdiction carve out certain processing activities from their material scope?

The UAE Law

The UAE Personal Data Protection Law carves out certain processing activities from its material scope, which are as follows:

- (a) Government data.
- (b) Processing or control of personal data by government authorities.
- (c) Personal data that is being processed/held by the security and judicial authorities.
- (d) A data subject who processes his or her personal data for personal purposes.
- (e) Personal health data that is subject to legislation regulating the protection and processing thereof.
- (f) Any processing of personal banking and credit data that has been done under the relevant legislation which govern the protection of this type of personal data.
- (g) The law is not applicable to companies and institutions situated in freezones and that are under the scope of special data privacy laws.

The DIFC Law

The DIFC Law carves out the natural persons from its material scope, as per the law, to which it does not apply to for the processing of personal data by natural persons, when such personal data processing is being carried out for purely household and personal purposes and does not involve any commercial purpose.

The ADGM Law

As per the ADGM Law, the following two categories have been excluded from its material scope:

- (a) The processing of personal data by a natural person for the purposes of purely personal or household activity.
- (b) When the processing of the personal data has been carried out by the public authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or for the execution of any criminal penalties. Also, when a public authority processes the personal data to safeguard against any anticipated threats to national security and also when such processing is carried out for the prevention of threats to national security.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

The key principles common in the UAE Law, the DIFC Law and the ADGM Regulations are:

- **Fairness, lawfulness and transparency**
Personal data must be processed fairly, lawfully and in a transparent manner.
- **Purpose limitation**
Personal data must be processed for a specified purpose.
- **Data adequacy**
Personal data must be adequate and limited to what is necessary in relation to the purpose of processing.
- **Accuracy**
Personal data must be accurate and updated.
- **Retention**
Once the purpose of processing is completed, personal data must be kept in a manner that does not permit identification of the data subject.
- **Security**
Personal data is to be processed ensuring security of the personal data, including unauthorised or unlawful processing and against accidental loss, destruction or damage by the use of appropriate technical and organisational measures.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

The following rights are available to individuals under the UAE Law, the DIFC Law and the ADGM Regulations:

- **Right to be informed**
A data subject is to be informed about the collection of his or her personal data, with certain specified information, irrespective of whether the personal data is received from the data subject or from any other source.
- **Right to access to (copies of) data/information about processing**
A data subject has the right to have confirmation and a copy of his or her personal data being processed by the controller.
- **Right to deletion/right to be forgotten**
A data subject has the right to have his or her personal data erased.

■ **Right to rectification**

A data subject has the right to have rectified inaccurate personal data or to complete the incomplete personal data.

■ **Right to data portability**

A data subject has the right to receive his or her personal data in a structured and commonly used machine-readable format and to transmit the personal data to another controller.

■ **Right related to automated decision-making and profiling**

A data subject has the right to not be subjected to a decision solely based on automated decision-making (without human intervention), including profiling.

■ **Right to withdraw consent**

A data subject has the right to withdraw his or her consent.

■ **Right to object**

A data subject has the right to object to the processing of his or her personal data, including when personal data is being used for direct marketing.

■ **Right to complain to the relevant data protection authority**

A data subject has the right to complain to the relevant personal data protection authority in case of any contravention of any of the legal provisions of the UAE Law/the DIFC Law/the ADGM Regulations.

5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

The data subjects have no right to mandate not-for-profit organisations to seek remedies on their behalf.

As regards collective redress, the UAE Law does not have such a provision; however, the DIFC Law and the ADGM Regulations permit class actions. Where multiple data subjects are affected by the same alleged contravention, they may raise a collective complaint. In addition, the Commissioner/Commissioner of Data Protection may choose to deal collectively with multiple allegations that relate to the same contravention, whether or not such allegations are brought collectively.

6 Children's Personal Data

6.1 What additional obligations apply to the processing of children's personal data?

The UAE Law, the DIFC Law and the ADGM Regulations do not address the processing of children's personal data.

7 Registration Formalities and Prior Approval

7.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

There is no requirement for the registration of controllers or processors under the UAE Law.

The DIFC Law requires that a controller or processor shall register with (and pay the prescribed fee to) the Commissioner.

The ADGM Regulations requires a controller to pay a data protection fee and notify (to the Commissioner of Data Protection) its name, address and the date it commenced processing personal data.

7.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

The DIFC Law provides that the notification must provide:

- A general description of the personal data processing being carried out.
- An explanation of the purpose of processing.
- The data subjects or class of data subjects whose personal data is being processed.
- A description of the class of personal data being processed.
- A statement of jurisdictions to which personal data will be transferred along with an indication as to whether the particular jurisdiction has been assessed as having an adequate level of protection.

The ADGM Regulations require a controller to notify, to the Commissioner of Data Protection, its name and address and the date it commenced processing personal data.

7.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

The DIFC Law requires the notification on a controller or processor basis.

The ADGM Regulations requires notification on a controller basis.

7.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

The DIFC Law requires that a controller or a processor must notify the Commissioner of the following processing operations, including but not limited to:

- processing of personal data;
- processing of special category data; and
- transfer of personal data to a recipient outside the DIFC which is not subject to laws and regulations that ensure an adequate level of protection.

The ADGM Regulations require that a controller, before or as soon as reasonably practicable, after it starts processing, notify the Commissioner of Data Protection.

7.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

As stated in question 7.2.

7.6 What are the sanctions for failure to register/notify where required?

The maximum fine, under the DIFC Law, for failure to register/notify is US\$ 25,000.

The ADGM Regulations do not provide for a specific sanction or fine for failure to register/notify. The maximum general administrative fine is up to US\$ 28 million for doing an act prohibited or to omit to do an act, under the ADGM Regulations.

7.7 What is the fee per registration/notification (if applicable)?

The fee for registration/notification under the DIFC Law ranges between US\$ 250 to US\$ 1,250.

The fee for ADGM is US\$ 300.

7.8 How frequently must registrations/notifications be renewed (if applicable)?

Both the DIFC Law and the ADGM Regulations require renewal on an annual basis.

7.9 Is any prior approval required from the data protection regulator?

Prior approval from the data protection regulator is not required.

7.10 Can the registration/notification be completed online?

The notification can be completed online, both for the DIFC and the DGM.

7.11 Is there a publicly available list of completed registrations/notifications?

Under the DIFC Law, the Commissioner is to keep the notifications on a publicly available register maintained by the Commissioner.

The information on ADGM registered controllers is available in the ADGM Public Register of companies.

7.12 How long does a typical registration/notification process take?

The time to process a notification, at the DIFC and ADGM, depends on the individual circumstances of each controller or processor (how detailed the information to be fed in is).

8 Appointment of a Data Protection Officer

8.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

- A Data Protection Officer (DPO) is required to be

appointed when the processing is likely to result in a high risk to the privacy and confidentiality of personal data, due to the adoption of new technologies or due to the amount of data.

- A DPO is required to be appointed where the processing involves a systematic and overall assessment of sensitive personal data, including profiling and automated processing.

The executive regulations will specify the kinds of technologies and standards of determination of the amount of data related to the above.

The DIFC Law

- A DPO is required to be appointed by the Commissioner, DIFC Authority and by the Dubai Financial Services Authority.
- A DPO is required to be appointed by a controller or processor performing high-risk activities on a systematic or regular basis.
- A controller or processor (other than above) may be required to designate a DPO by the Commissioner.

The ADGM Regulations

- A DPO is required to be appointed where processing is carried out by a public authority except for courts acting in their judicial capacity.
- A DPO is required to be appointed where core activities of a controller or processor require (on the basis of nature, scope and purposes of processing) regular and systematic monitoring of data subjects on a large scale.
- A DPO is required to be appointed where core activities of a controller or processor consist of processing of a large scale or special categories of personal data.

8.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

The sanctions/fines under the UAE Law are yet to be prescribed.

Under the DIFC Law, the maximum fine for failure to appoint a DPO is US\$ 50,000.

The ADGM Regulations do not provide for a specific sanction or fine for failure to appoint a DPO. The maximum general administrative fine is up to US\$ 28 million for carrying out a prohibited act or omitting to do an act, under the ADGM Regulations.

8.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

The UAE Law, the DIFC Law and the ADGM Regulations do not provide any such protection.

8.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

The UAE Law has no such provision.

The DIFC Law and the ADGM Regulations do allow appointment of a single DPO by a group, provided that the DPO is easily accessible from each entity in the group.

8.5 Please describe any specific qualifications for the Data Protection Officer required by law.

There are no specified qualifications for the appointment of a DPO. The general requirement is having adequate skills and knowledge with the applicable data protection law.

8.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

The responsibilities of a DPO, among others, include:

- Monitoring the compliance of the controller or processor within the applicable legal framework.
- Informing and advising the controller, processor and their respective employees (who carry out personal data processing) about their obligations under the applicable legal framework.
- Acting as the contact point for the concerned regulator.

8.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

- Under the UAE Law, the controller or processor is to designate the contact details of the DPO and inform the UAE Data Office.
- There is no such requirement under the DIFC Law.
- The ADGM Regulations require that the controller or processor must notify the appointment of a DPO, within one month of appointment, to the Commissioner of Data Protection.

8.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

There is no such requirement under the UAE Law or the ADGM Regulations.

The DIFC Law requires that a controller or processor shall publish the contact details of its DPO in a manner that is readily accessible to third parties.

9 Appointment of Processors

9.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

The UAE Law requires that controllers are to appoint processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that provisions of the UAE Law could be met.

The DIFC Law/the ADGM Regulations

The processing by a processor is to be governed by a legally binding written agreement between the controller and processor. A processor is to provide sufficient assurances/guarantees to implement appropriate technical and organisational measures to ensure that processing meets the legal requirements and to ensure the protection of rights of the data subjects.

9.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

- **The UAE Law:** The processor is to process the personal data upon instructions from the controller and pursuant to the contract between the controller and processor. The said contract is to identify scope, subject, purpose, nature and type of personal data and categories of data subject.
- **The DIFC Law/the ADGM Regulations:** The agreement between the controller and processor is to contain, among others:

The DIFC Law	The ADGM Regulations
Subject-matter and duration of the processing. Nature and purpose of the processing. Type of personal data and categories of data subjects. Obligations and rights of the controller. Commitment by the processor to process personal data based on documented instructions from the controller. Ensuring that persons authorised to process relevant personal data are under legally binding written agreements or duties of confidentiality.	The processor is to process the personal data only on documented instructions from the controller. Ensuring that persons authorised to process the personal data have committed themselves to confidentiality. Taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures. At the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services.

10 Marketing

10.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

The TDRA has outlined the “Regulatory Policy for Spam Electronic Communications” (Policy). The Policy requires that licensees (of the TDRA) are to put all practical measures in place to minimise the transmission of spam having a UAE link across their telecommunication networks. The Policy further states that licensees shall not sell, supply, use or knowingly allow access or right to use any tools, software, hardware or mechanisms that facilitate the harvesting and generation of electronic addresses.

10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

The above-mentioned policy does not differentiate as to business-to-consumer or business-to-business.

10.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

Please refer to question 10.1.

10.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?

The above-mentioned policy is applicable only to licensees of the TDRA.

10.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

No such information is available.

10.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

The purchase of marketing lists from third parties is not addressed in the UAE Law, the DIFC Law or the ADGM Regulations.

10.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

The penalties under the UAE Law are yet to be prescribed.

The DIFC Law and the ADGM Regulations do not specifically provide for a penalty for sending marketing communications in breach of applicable restrictions.

11 Cookies

11.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

- The UAE Law confers on the data subject a “right to stop processing” where personal data is processed for direct marketing purposes, including profiling to the extent that profiling is related to such direct marketing.
- The DIFC Law provides that a data subject has the right to be informed before personal data is disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing and that the data subject be expressly offered the right to object to direct marketing. The data subject has the right to object to personal data processing for direct marketing purposes, including profiling to the extent that such profiling is related to direct marketing.
- The ADGM Regulations carry the same provisions as in the DIFC Law regarding direct marketing. The ADGM Regulations, in addition, provide that when a data subject objects to direct marketing, personal data must not be processed for direct marketing purposes.

11.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

The restrictions, as stated above, do not distinguish between different types of cookies.

11.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

No such information is available.

11.4 What are the maximum penalties for breaches of applicable cookie restrictions?

The penalties under the UAE Law are yet to be prescribed.

The DIFC Law and the ADGM Regulations do not specifically provide for a penalty for breach of applicable cookie restrictions.

12 Restrictions on International Data Transfers

12.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

The UAE Law

The UAE Law provides that personal data may only be transferred outside the UAE to a jurisdiction that has a law in place covering various aspects as to the protection of personal data (adequate level of protection). The personal data may also be transferred to those countries with whom the UAE has bilateral or multilateral agreements in respect of personal data protection.

In the absence of an adequate protection, under the UAE Law, personal data may be transferred outside the UAE in the following cases (subject to the controls to be specified by the executive regulations):

- In jurisdictions where data protection law does not exist, on the basis of a contract or agreement binding the establishment (to whom personal data is being transferred) to follow the provisions, measures, controls and conditions of the UAE Law. The said contract or agreement must also specify a supervisory or judicial entity in that foreign country for imposition of appropriate measures against the controller or processor in that foreign country.
- Expressed consent of the data subject, in such a manner that does not conflict with the public and security interest of the UAE.
- Transfer is necessary for performing obligations and establishing rights before judicial entities.
- Transfer is necessary for entering or performance of a contract between the controller and the data subject, or between the controller and a third party for the interests of the data subject.
- Transfer is necessary for the performance of an act relating to international judicial cooperation.
- Transfer is necessary for the protection of public interest.

The DIFC Law

The DIFC Law provides that personal data may be transferred abroad on the basis of adequate level of protection as

determined by the Commissioner. A list of adequate jurisdictions is issued through the DIFC Data Protection Regulations.

The ADGM Regulations

The ADGM Regulations permit transferring personal data abroad where the Personal Data Commissioner has decided that the receiving jurisdiction ensures an adequate level of protection. A list of jurisdictions designated as having an adequate level of protection is available at the ADGM website.

Transfer on the Basis of Appropriate Safeguards – The DIFC Law and the ADGM Regulations

In the absence of an adequate level of protection, personal data may be transferred abroad on the basis of “appropriate safeguards”. The “appropriate safeguards” include:

- A legally binding instrument between the public authorities.
- Binding corporate rules.
- Standard data protection clauses.
- Approved code of conduct.
- Approved certification mechanism.

Specific Derogations – The DIFC Law and the ADGM Regulations

In the absence of an adequate level of protection and appropriate safeguards, the data may be transferred outside under the following derogations:

- Explicit consent of the data subject.
- Transfer is necessary for the performance of a contract between the data subject and controller.
- Transfer is necessary for the conclusion or performance of a contract between a controller and a third party which is in the interest of the data subject.
- Transfer is necessary for reasons of public interest.
- Transfer is necessary in accordance with an applicable law.
- Transfer is necessary for establishment, exercise or defence of a legal claim.
- Transfer is necessary to protect the vital interests of a data subject or of other persons where a data subject is physically or legally incapable of giving consent.
- Transfer is made in compliance with applicable law and data minimisation principles to provide information to the public, and is open for viewing by the public in general or by a person who can demonstrate a legitimate interest (under the DIFC Law only).
- Transfer is necessary for compliance with any obligation under applicable law to which the controller is subject, or transfer is made at the reasonable request of a regulator, police or other government agency or competent authority (under the DIFC Law only).
- Transfer is necessary to uphold the legitimate interests of a controller (in international financial markets), subject to international financial standards, except where such interests are overridden by the legitimate interest of the data subject (under the DIFC Law only).
- Transfer is necessary to comply with the anti-money laundering or counter-terrorist-financing obligations applicable to a controller or a processor (under the DIFC Law only).

12.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g.,

consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

Please refer to question 12.1.

12.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

Under the DIFC Law, in the absence of an adequate level of protection, absence of appropriate safeguards and absence of derogations, the personal data may be transferred outside only if:

- the transfer is not repeating or part of a repetitive course of transfers;
- the transfer concerns only a limited number of data subjects;
- the transfer is necessary for the purpose of compelling legitimate interests pursued by the controller that are not overridden by the interests or rights of the data subject; and
- the controller has completed a documentary assessment of all circumstances surrounding data transfer and has on the basis of such an assessment provided suitable safeguards for the protection of personal data.

In the above case, the controller is to inform the Commissioner and also inform the data subject about the transfer and the controllers’ compelling legitimate interests.

12.4 Do transfers of personal data to other jurisdictions require a transfer impact assessment? If conducting a transfer impact assessment is only mandatory in some circumstances, please identify those circumstances.

The DIFC Law/ADGM Regulations: where a controller or processor will receive a request from any public authority over the person, for the disclosure and transfer of any personal data, the controller or processor should assess the impact of the proposed transfer in light of the potential risks to the right of any affected data subject and, where appropriate, implement measures to minimise risks, including by redacting or minimising the personal data transferred to the extent possible or utilising appropriate technical or other measures to safeguard the transfer of personal data.

12.5 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?

- In light of the *Schrems II* case followed by the US–EU Trans-Atlantic Data Privacy Framework: the DIFC has guided that in case a DIFC entity is part of a multinational or group business that engages in transfers/onward transfers from the EU, then the DIFC entity is to ensure (once personal data leaves the DIFC for processing in the EU) that transfers remain compliant with Article 27 of the DIFC Law (transfers outside the DIFC in the absence of an adequate level of protection).

- The ADGM Office of Data Protection has invalidated the EU-US Privacy Shield and confirmed that the ADGM will not continue to recognise the Shield as a legitimate transfer mechanism.

12.6 What guidance (if any) has/have the data protection authority(ies) issued in relation to the use of standard contractual/model clauses as a mechanism for international data transfers?

No guidance has been issued.

13 Whistle-blower Hotlines

13.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

The concept of whistle-blowing is not addressed in the UAE Law, the DIFC Law or the ADGM Regulations.

13.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

None, in view of the answer to question 13.1.

14 CCTV

14.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

The use of CCTV is not addressed in the UAE Law, the DIFC Law or the ADGM Regulations.

14.2 Are there limits on the purposes for which CCTV data may be used?

None, in view of the answer to question 14.1.

15 Employee Monitoring

15.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Employee monitoring is not addressed in the UAE Law, the DIFC Law or the ADGM Regulations.

15.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

None, in view of the answer to question 15.1.

15.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

None, in view of the answer to question 15.1.

15.4 Are employers entitled to process information on an employee's attendance in office (e.g., to monitor compliance with any internal return-to-office policies)?

It is stipulated in all three laws that a Controller (herein "employer") can process the personal data of the data subject ("employee") for the execution of the contract to which the data subject is party to. An employer, while entering into an employment contract with the employee wherein it is mentioned that the employer can monitor the employee's attendance, is entitled to process the personal data of the employee.

16 Data Security and Data Breach

16.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

The UAE Law

The controller and processor are to put in place and implement appropriate technical and organisational measures and actions to ensure a high security level which is appropriate to the risks associated with the processing. These measures are to be in accordance with the best international standards and practices.

The DIFC Law/the ADGM Regulations

The controllers (and processors also under the DIFC Law) are required to implement appropriate technical and organisational measures to protect personal data. In addition, the controllers are required to ensure the security of personal data by following the principles of "data protection by design" and "data protection by default".

16.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

The data controller is required to notify a data breach to the Data Office/Commissioner/Commissioner of Data Protection when the breach is likely to result in a risk to the privacy, confidentiality, security or rights of the data subjects. The processor is to notify, without delay, any such breach to the controller.

The UAE Law requires to notify the breach immediately. The DIFC Law requires to notify the breach as soon as practicable in the circumstances. The ADGM Regulations provides that breach notification be made within 72 hours after having become aware of the breach, and, in case the notification is not reported within 72 hours, then reasons of delay must also accompany the breach notification.

The breach notification is to contain at least the following information:

- description of the nature of the breach;
- details of the DPO;
- likely effects/consequences of the breach;
- description of measures taken or proposed to be taken by the controller to rectify/remedy the breach and the measures to mitigate its effects; and
- any other requirement of the Data Office (only in case of the UAE Law).

16.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Where a breach is likely to result in a high risk to the security or rights of a data subject, the controller is required to also notify the breach to the data subject. In that case, the reporting requirements and timeframe are the same as those mentioned at question 16.2.

16.4 What are the maximum penalties for personal data security breaches?

The penalties under the UAE Law are yet to be prescribed. Under the DIFC Law, the maximum fine for failure to implement and maintain technical and organisational measures to protect personal data is US\$ 50,000. The ADGM Regulations do not provide for a specific sanction or fine for data security breaches. The maximum general administrative fine is up to US\$ 28 million for carrying out a prohibited act or to omit to carry out an act, under the ADGM Regulations.

17 Enforcement and Sanctions

17.1 Describe the enforcement powers of the data protection authority(ies).

The UAE Law

The UAE Data Office is responsible for enforcing data privacy under the UAE Law. The UAE Data Office is competent to receive and decide the complaints of data subjects regarding contravention of the provisions of the UAE Law. The Data Office is also competent to impose administrative sanctions.

The DIFC Law

The Commissioner (DIFC) administers the DIFC Law. The Commissioner (DIFC) is empowered to receive and decide complaints concerning the contravention of the DIFC Law. The Commissioner (DIFC) is also empowered to investigate complaints and to issue directions or declarations on the complaints and impose fines.

The ADGM Regulations

The Commissioner of Data Protection for the ADGM (the ADGM Commissioner) is responsible for enforcement of the ADGM Regulations. The ADGM Commissioner is empowered to receive and decide complaints regarding the contravention

of the ADGM Regulations and to impose fines. The ADGM Commissioner is also competent to carry out investigations and to issue directions.

17.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The UAE Data Office has no such powers. The Commissioner (DIFC) is empowered to issue directions to refrain from processing personal data specified in the direction, for a purpose or in a manner specified in the direction. A court order is not required in this regard. The Commissioner of Data Protection (ADGM) has the power to impose a temporary or permanent limitation (including a ban) on the processing. A court order is not required in this regard.

17.3 Describe the data protection authority’s approach to exercising those powers, with examples of recent cases.

No such information is available.

17.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

No such information is available.

18 E-discovery/Disclosure to Foreign Law Enforcement Agencies

18.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Foreign e-discovery requests are responded to considering the relevant circumstances in each particular case.

18.2 What guidance has/have the data protection authority(ies) issued on disclosure of personal data to foreign law enforcement or governmental bodies?

No guidance has been issued in this regard.

19 Artificial Intelligence

19.1 Are there any limitations on automated decision-making involving the processing of personal data using artificial intelligence?

The ADGM Regulations impose certain limitations on the processing of personal data by the use of automated means; a data subject is vested with the right to not be subject to decisions based solely on automated processing. The DIFC Law has also imposed restrictions on processing by automated means. AI comes within the ambit of automated processing, which is defined in the Federal Decree Law as: “A processing operation which is performed using [an] electronic system or program

operating in an automated manner, either in a complete autonomous way without any human intervention or partially under limited human supervision and intervention.”

The Federal Decree Law has also given this right to the data subject that he/she shall have the authority to object to automated decision-making that has legal implications or seriously affects the data subject.

19.2 What guidance (if any) has/have the data protection authority(ies) issued in relation to the processing of personal data in connection with artificial intelligence?

The DIFC has introduced specific guidelines in terms of Regulation 10, addressing AI and personal data processing. This regulation mandates that individuals must be informed when their data is processed by autonomous or semi-autonomous systems, such as AI. As per these regulations, where advanced technology is deployed that does not permit the exercise of data subjects’ rights such as erasure, the

deployer/controller must provide sufficient notice in that regard and satisfy itself that the data subjects understand the impact.

20 Trends and Developments

20.1 In your opinion, what enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.

No details are available concerning enforcement trends.

20.2 In your opinion, what “hot topics” are currently a focus for the data protection regulator?

Executive regulations pursuant to the UAE Law are to be announced, which will provide procedural aspects with respect to matters provided for in the UAE Law.



Saifullah Khan is an international trade, IT and policy lawyer with more than 20 years of diversified and multi-jurisdictional professional experience serving a large client base in the domestic and international markets. His areas of interest include trade remedy laws of the World Trade Organization, customs law, competition law and data privacy. With respect to emerging discipline of data privacy, he advises clients from different jurisdictions on data privacy compliance and cross-border transfer of data. Additionally, he assists clients in the preparation and review of privacy policies and intra-group agreements concerning cross-border transfer of personal data, etc. He is an advocate of the High Court, a member of the Chartered Institute of Arbitrators (UK) and a member of the International Association of Privacy Professionals. He has completed a course at the London School of Economics and Political Science on "Data: Law, Policy and Regulation".

Bizilance Legal Consultants

D 3-4, Office 302
Al Sarab Tower, Level 15
ADGM Abu Dhabi
United Arab Emirates

Tel: +971 58 184 8960
Email: saifullah.khan@bizilancelegal.ae
LinkedIn: www.linkedin.com/in/saifullahkhan



Saeed Hasan Khan has more than 20 years' experience advising clients on issues such as taxation, corporate, regulatory compliance and contractual obligations, and in representing clients before the authorities. Mr. Khan has developed a keen professional interest in emerging laws on personal data protection and has gained an understanding of the underlying concepts and principles governing global data protection laws, including the EU's General Data Protection Regulation. He has carried out a great deal of research on personal data protection laws in various jurisdictions in order to compare their core legal principles. He is an advocate of the High Court, a member of the Chartered Institute of Arbitrators (UK) and a member of the International Association of Privacy Professionals. He has completed a course from the London School of Economics and Political Science on "Data: Law, Policy and Regulation".

Bizilance Legal Consultants

D 3-4, Office 302
Al Sarab Tower, Level 15
ADGM Abu Dhabi
United Arab Emirates

Tel: +971 52 914 1118
Email: saeed.hasan@bizilancelegal.ae
LinkedIn: www.linkedin.com/in/saeed-hasan-khan-1338a63a

Bizilance Legal Consultants practises trade remedy laws, privacy and data protection, taxation, and antitrust and competition, among others. The firm is backed by the rich experience of its partners, spread over two decades. The partners have served clients in multiple jurisdictions, including the UAE, the USA, the UK, Switzerland, Singapore, China, Malaysia, Indonesia, Korea, Thailand and Pakistan. In the personal data and privacy space, Bizilance Legal Consultants at Abu Dhabi Global Market is strategically well placed to serve multi-jurisdictional clients in an era when laws related to personal data protection have either just been implemented or are in the process of being implemented.

www.bizilancelegal.ae



United Kingdom

White & Case LLP



Tim Hickman



Aishwarya Jha

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

Until the UK's departure from the EU, and the end of the "Transition Period" on 31 December 2020, the principal data protection legislation in the UK was Regulation (EU) 2016/679 (the "**General Data Protection Regulation**" or "**GDPR**"). The GDPR repealed Directive 95/46/EC (the "**Data Protection Directive**") and led to increased (though not total) harmonisation of data protection law across the EU Member States. Some provisions in the GDPR can be adapted in EU Member States' national laws. Therefore, the UK Government passed the Data Protection Act 2018, and several subsequent amendments (the "**DPA 2018**"), which cover those areas of the GDPR that EU Member States could add to or vary or that do not fall within EU law. The DPA 2018 came into force on 25 May 2018.

Following the UK's departure from the EU, the GDPR was incorporated into the domestic law that applies in the UK, under Section 3 of the European Union (Withdrawal) Act 2018 (the "**Withdrawal Act**"), and the DPA 2018, as amended by the Data Protection, Privacy and Electronic Communications (Amendments, etc.) (EU Exit) Regulations 2019. The amended GDPR (the "**UK GDPR**") and the DPA 2018 are now the principal pieces of data protection legislation in the UK.

The UK GDPR is broadly aligned with the GDPR in terms of its substantive requirements. However, the provisions concerning supervisory bodies and interactions between EU Member States have been amended to reflect the fact that the UK is no longer directly subject to EU law and enforcement regimes. Powers previously held at the EU level are now held by the UK's Information Commissioner.

References to "UK GDPR" used throughout this chapter should be read to include "DPA 18".

1.2 Is there any other general legislation that impacts data protection?

The Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended from time to time) (the "**PECR**") implement the requirements of Directive 2002/58/EC (as amended by Directive 2009/136/EC) (the "**ePrivacy Directive**"), which provides a specific set of privacy rules to harmonise the processing of personal data by the telecoms sector. The PECR remain in force following the UK's departure from the EU.

The Data Protection and Digital Information (No.2) Bill (the "**Data Protection Bill**"), introduced in March 2023, had proposed several changes to the UK GDPR, the DPA 2018 and the PECR (among other laws). However, the Data Protection Bill was not completed in light of the UK's 2024 General Election, and failed to become legislation prior to the dissolution of the Parliament. In its stead, the Data (Use and Access) Bill (the "**DUA Bill**") was introduced in October 2024. The DUA Bill (discussed in more detail in question 20.2) largely builds upon the Data Protection Bill and is set to reform the UK's legislative and regulatory regime relating to the use of, and access to, data, in an effort to enable data-driven innovation and growth. At the time of writing, the DUA Bill is in its final stages, and is expected to come into force in early 2026.

1.3 Is there any sector-specific legislation that impacts data protection?

No, there is no sector-specific legislation that impacts data protection.

1.4 What authority(ies) are responsible for data protection?

The Information Commissioner's Office (the "**ICO**") is responsible for overseeing and enforcing the UK GDPR and the PECR in the UK. It is an independent body, which is sponsored by the Department for Digital, Culture, Media and Sport and reports directly to Parliament. In January 2022, John Edwards was appointed Information Commissioner.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**"
Any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- "**Processing**"
Any operation or set of operations which is performed on personal data or on sets of personal data, whether or

not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

- **“Controller”**
The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- **“Processor”**
A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- **“Data Subject”**
An individual who is the subject of the relevant personal data.
- **“Special Categories of Personal Data”**
This includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health, sex life or sexual orientation, genetic data or biometric data. Special categories of personal data together with personal data relating to criminal convictions and offences are sometimes referred to as “sensitive personal data”.
- **“Data Breach”**
A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
- **“Profiling”**
Any form of automated processing of personal data consisting of the use of personal data to evaluate certain aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

3 Territorial and Material Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The UK GDPR applies to businesses that are established in the UK, and that process personal data (either as a controller or processor, and regardless of whether or not the processing takes place in the UK) in the context of that establishment.

A business that is not established in the UK, but is subject to the laws of the UK by virtue of public international law, is also subject to the UK GDPR.

The UK GDPR applies to businesses outside the UK if they (either as controller or processor) process the personal data of UK residents in relation to: (i) the offering of goods or services (whether or not in return for payment) to UK residents; or (ii) the monitoring of the behaviour of UK residents (to the extent that such behaviour takes place in the UK).

3.2 Do the data protection laws in your jurisdiction carve out certain processing activities from their material scope?

The UK GDPR explicitly excludes certain activities from its scope. In particular, any activity performed by a natural person in the course of a purely personal or household activity is outside the material scope of the UK GDPR. As another example, any processing of personal data by a competent authority for law enforcement purposes is also outside the material scope of the UK GDPR.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
Personal data must be processed lawfully, fairly and in a transparent manner. Controllers must provide certain minimum information to data subjects regarding the collection and further processing of their personal data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
- **Lawful basis for processing**
Processing of personal data is lawful only if, and to the extent that, it is permitted under UK data protection law. The UK GDPR provides an exhaustive list of legal bases on which personal data may be processed, of which the following are the most relevant for businesses: (i) prior, freely given, specific, informed and unambiguous consent of the data subject; (ii) contractual necessity (i.e., the processing is necessary for the performance of a contract to which the data subject is a party, or for the purposes of pre-contractual measures taken at the data subject’s request); (iii) compliance with legal obligations (i.e., the controller has a legal obligation, under the laws of the UK, to perform the relevant processing); or (iv) legitimate interests (i.e., the processing is necessary for the purposes of legitimate interests pursued by the controller, except where the controller’s interests are overridden by the interests, fundamental rights or freedoms of the affected data subjects).
Please note that businesses require stronger grounds to process special categories of personal data. The processing of special categories of personal data is only permitted under certain conditions, of which the most relevant for businesses are: (i) explicit consent of the affected data subject; (ii) the processing is necessary in the context of employment law; or (iii) the processing is necessary for the establishment, exercise or defence of legal claims. The processing of personal data relating to criminal convictions and offences is only permitted where it takes place under the control of official authority, or is authorised by applicable law in the UK.
- **Purpose limitation**
Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes. If a controller wishes to use the relevant personal data in a manner that is incompatible with the purposes for which they were initially collected, it must: (i) inform the data subject of such new processing; and (ii) be able to rely on a lawful basis as set out above.

- **Data minimisation**
Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed. A business should only process the personal data that it actually needs to process in order to achieve its processing purposes.
- **Proportionality**
This is not applicable.
- **Retention**
Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- **Accuracy**
Personal data must be accurate and, where necessary, kept up to date. A business must take every reasonable step to ensure that personal data that are inaccurate are either erased or rectified without delay.
- **Data security**
Personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- **Accountability**
The controller is responsible for, and must be able to demonstrate, compliance with the data protection principles set out above.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to (copies of) data/information about processing**
A data subject has the right to obtain from a controller the following information in respect of the data subject's personal data: (i) confirmation of whether, and where, the controller is processing the data subject's personal data; (ii) information about the purposes of the processing; (iii) information about the categories of data being processed; (iv) information about the specific recipients or categories of recipients with whom the data may be shared; (v) information about the period for which the data will be stored (or the criteria used to determine that period); (vi) information about the existence of the rights to erasure, to rectification, to restriction of processing and to object to processing; (vii) information about the existence of the right to complain to the relevant data protection authority; (viii) where the data were not collected from the data subject, information as to the source of the data; and (ix) information about the existence of, and an explanation of the logic involved in, any automated processing that has a legal or other significant effect on the data subject.
Additionally, the data subject may request a copy of the personal data being processed, to the extent that the personal data requested does not adversely affect the rights and freedoms of others.
- **Right to rectification of errors**
Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data subjects have the right to rectification of inaccurate personal data.
- **Right to deletion/right to be forgotten**
Data subjects have the right to erasure of their personal data (the right to be forgotten) if: (i) the data are no longer needed for their original purpose (and no new lawful purpose exists); (ii) the lawful basis for the processing is the data subject's consent, the data subject withdraws that consent, and no other lawful ground exists; (iii) the data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing; (iv) the data have been processed unlawfully; or (v) erasure is necessary for compliance with UK law.
- **Right to object to processing**
Data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data where the basis for that processing is either public interest or legitimate interest of the controller. The controller must cease such processing unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the relevant data subject or it requires the data in order to establish, exercise or defend legal rights.
- **Right to restrict processing**
Data subjects have the right to restrict the processing of personal data, which means that the data may only be held by the controller, and may only be used for limited purposes if: (i) the accuracy of the data is contested (and only for as long as it takes to verify that accuracy); (ii) the processing is unlawful and the data subject requests restriction (as opposed to exercising the right to erasure); (iii) the controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights; or (iv) verification of overriding grounds is pending, in the context of an erasure request.
- **Right to data portability**
Data subjects have a right to receive a copy of their personal data in a commonly used machine-readable format, and to transfer their personal data from one controller to another or have the data transmitted directly between controllers.
- **Right to withdraw consent**
A data subject has the right to withdraw their consent at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject must be informed of the right to withdraw consent. It must be as easy to withdraw consent as it is to give it.
- **Right to object to marketing**
Data subjects have the right to object to the processing of personal data for the purpose of direct marketing, including profiling.
- **Right protecting against solely automated decision-making and profiling**
Data subjects have the right to not be subject to a decision based solely on automated processing (including profiling) that produces legal effects (or similarly significant effects). This restriction does not apply if the decision: (i) is necessary for entering into, or performance of, a contract between the data subject and the controller; (ii) is authorised by UK law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or (iii) is based on the data subject's explicit consent. In the case of (i)–(iii), the controller is required to implement suitable measures to safeguard

the data subject’s rights, freedoms and legitimate interests, including at least the right to obtain human intervention on the part of the controller, so that the data subject is able to express their point of view and to contest decisions reached.

- **Right to complain to the relevant data protection authority(ies)**
Data subjects have the right to lodge complaints concerning the processing of their personal data with the ICO, if the data subject lives in the UK or the alleged infringement occurred in the UK.
- **Right to basic information**
Data subjects have the right to be provided with information on the identity of the controller, the reasons for processing their personal data and other relevant information necessary to ensure the fair and transparent processing of personal data.
- **Right to compensation**
Data subjects who have suffered (material or non-material) damage as a result of the unlawful processing of their personal data have the right to receive compensation from the relevant controller and/or processor for the harm suffered.

5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

Yes, data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or to seek collective redress.

6 Children’s Personal Data

6.1 What additional obligations apply to the processing of children’s personal data?

Article 8(1) of the UK GDPR provides that in order to offer an “information society service” (“ISS”) to a child under the age of 13 years old on the basis of consent, such consent must be given or authorised by the child’s parent or guardian.

An ISS is defined as “any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services”, and therefore most online services are ISSs (e.g., social media services, online gaming and web-based voice, video and text messaging).

The interpretation of “remuneration” in this context is broad, and is triggered even if the end-users themselves do not pay for the services, but the service provider relies on advertising revenue to fund the services.

In September 2021, the ICO’s Age Appropriate Design Code (the “AADC”) took effect. The purpose of the AADC is to help ensure that service providers put the best interests of children first when designing any ISS. In order to achieve this aim, the AADC sets out 15 standards with which businesses that provide ISSs to children in the UK should comply. These include standards on, among other things: (i) data protection impact assessments (“DPIAs”); (ii) transparency; (iii) detrimental use of data; (iv) policies and community standards; (v) default settings; (vi) data sharing; (vii) parental controls; and (viii) connected toys and devices.

7 Registration Formalities and Prior Approval

7.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

No, there is no longer a legal obligation on businesses to register with or notify the ICO as there was under the Data Protection Act 1998. This requirement has been replaced by a legal obligation on controllers (not processors) to pay a data protection fee under the Data Protection (Charges and Information) Regulations 2018, which came into force on 25 May 2018. As such, the following questions in this section will relate to the fee requirement instead of the registration requirement. It should be noted that certain businesses are exempt, such as public authorities, charities and small occupational pension schemes.

In addition to the above, a controller must keep records of its processing activities which, upon request, must be disclosed to the ICO. Furthermore, a processor must keep records of its processing activities performed on behalf of a controller.

7.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

The information provided to the ICO need not be too detailed. Only the information listed in question 7.5 must be provided.

7.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

A separate fee is payable by every UK entity that acts as a controller.

7.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

Any controller that is subject to the DPA 2018 must pay the fee to the Information Commissioner unless it is exempt.

7.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

A controller must provide the ICO with the following information: contact details; number of staff; turnover for its financial year; type of organisation; and details of the Data Protection Officer (if applicable).

7.6 What are the sanctions for failure to register/notify where required?

The penalty for failing to pay the fee or paying the incorrect fee can be a maximum of 150% of the top-tier fee (see question 7.7 below).

7.7 What is the fee per registration/notification (if applicable)?

There are three tiers of fees ranging from £52 to £3,763 (note that the fees were revised by the UK Government in February 2025), and the fee payable depends on the size of the business, its turnover and the type of business.

7.8 How frequently must registrations/notifications be renewed (if applicable)?

The fee is payable annually.

7.9 Is any prior approval required from the data protection regulator?

No, prior approval is not required.

7.10 Can the registration/notification be completed online?

Payment of the fee can be completed online through the ICO's website.

7.11 Is there a publicly available list of completed registrations/notifications?

Yes, there is a public register of controllers who pay the data protection fee.

7.12 How long does a typical registration/notification process take?

As payment can be completed online through the ICO website, this process can be immediate. Other payment methods (e.g., cheques) may be slower.

8 Appointment of a Data Protection Officer

8.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The appointment of a Data Protection Officer for controllers or processors is only mandatory in some circumstances, including where there is: (i) large-scale regular and systematic monitoring of individuals; or (ii) large-scale processing of special categories of personal data.

Where a business designates a Data Protection Officer voluntarily, the qualification requirements for, and responsibilities of, Data Protection Officers under the UK GDPR (as described

in questions 8.5 and 8.6) apply as though the appointment were mandatory.

8.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

In the circumstances where appointment of a Data Protection Officer is mandatory, failure to comply may result in the wide range of penalties available under the UK GDPR.

8.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

The appointed Data Protection Officer should not be dismissed or penalised for performing their tasks, and should report directly to the highest management level of the controller or processor.

8.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

A group of undertakings may appoint a single Data Protection Officer, provided that the Data Protection Officer is easily accessible from each establishment.

8.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The Data Protection Officer should be appointed on the basis of professional qualities and should have an expert knowledge of data protection law and practices. While this is not strictly defined, it is clear that the level of expertise required will depend on the circumstances. For example, the involvement of large volumes of special categories of personal data will require a higher level of knowledge.

8.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

A Data Protection Officer should be involved in all issues that relate to the protection of personal data. The UK GDPR outlines the minimum tasks required by the Data Protection Officer, which include: (i) informing the controller/processor, including their relevant employees, who processes personal data, of their obligations under the UK GDPR; (ii) monitoring compliance with the UK GDPR, other national data protection legislation and internal policies in relation to the processing of personal data, including internal audits; (iii) advising on DPIAs and the training of staff; and (iv) co-operating with the ICO and acting as the primary contact point for the purposes of the ICO on issues related to the processing of personal data by the relevant entity.

8.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

Yes, the controller or processor must notify the data protection authority of the contact details of the designated Data Protection Officer.

8.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

The Data Protection Officer does not necessarily need to be named in the public-facing privacy notice. However, the contact details of the Data Protection Officer must be notified to the data subject when personal data relating to that data subject are collected. As a matter of good practice, the Article 29 Working Party (the “WP29”) (now the European Data Protection Board (the “EDPB”)) recommended in its 2017 guidance on Data Protection Officers that both the data protection authority and employees should be notified of the name and contact details of the Data Protection Officer. This guidance is likely to remain persuasive despite the UK’s departure from the EU.

9 Appointment of Processors

9.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes. The business that appoints a processor to process personal data on its behalf is required to enter into an agreement with the processor which sets out the subject matter for processing, the duration of processing, the nature and purpose of processing, the types of personal data and categories of data subjects, and the obligations and rights of the controller (i.e., the business).

It is essential that the processor appointed by the business complies with the UK GDPR.

9.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The processor must be appointed under a binding agreement in writing. Article 28(3) of the UK GDPR stipulates a minimum standard for the contractual terms to be entered into with each processor, which includes terms to ensure that the processor: (i) only acts on the documented instructions of the controller; (ii) imposes confidentiality obligations on individuals authorised to process the affected personal data; (iii) ensures the security of the personal data that it processes; (iv) abides by the rules regarding the appointment of sub-processors; (v) implements measures to assist the controller in giving effect to the rights of affected data subjects; (vi) assists the controller in obtaining approval from the ICO where required; (vii) either returns or destroys the personal data at the end of the relationship (except as required by UK law); and (viii) provides the controller with all the information necessary to demonstrate compliance with the UK GDPR.

10 Marketing

10.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

The PECR requires businesses to obtain consent before sending electronic communications to individuals for the

purpose of direct marketing. There are exemptions to this; however, they are very narrow.

10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

There are no specific restrictions applicable in a business-to-business context, although it is good practice for businesses to offer an opt-out of electronic direct marketing, such as emails or text messages, to other corporate bodies.

10.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

The PECR does not generally prohibit unsolicited marketing calls. However, the UK offers an opt-out register (the Telephone Preference Service (the “TPS”)). It is a legal requirement not to make unsolicited marketing calls to numbers registered in the TPS, without the consent of the relevant individual subscriber.

10.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?

The PECR does not have formal extraterritoriality provisions and therefore cannot be applied where there is no nexus with the UK.

10.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

Yes. The ICO has issued a number of fines to companies that breached direct marketing laws. Since 2018, there has been significant focus on “nuisance calls”. In 2024, the fines for contacting individuals without their consent ranged from £30,000 to £240,000. So far in 2025, the ICO has issued a fine of £90,000 to companies for non-compliance concerning unsolicited direct marketing.

In February 2025, the ICO launched its “direct marketing advice generator” to help provide organisations with guidance on how to comply with the PECR and the UK GDPR in respect of their direct marketing activities.

10.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

For a lawful purchase of a marketing list, the relevant individuals must have been originally informed by the seller that their data could be passed on to other businesses for marketing purposes and the individuals must have consented to that. The ICO recommends due diligence on any lists prior to purchase, and in practice, it is recommended that warranties are sought to ensure that the marketing list does not contravene applicable requirements.

10.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

The maximum fine under the PECR is £500,000, although typical fines are generally well below this level (with the exception of a few cases (e.g., in 2020, the ICO issued a fine to a company for the maximum amount for making more than 193 million automated “nuisance calls” to individuals)).

11 Cookies

11.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

The PECR implements Article 5 of the ePrivacy Directive. Pursuant to Article 5 of the EU ePrivacy Directive, the storage of cookies (or other data) on an end-user’s device requires prior consent (the applicable standard of consent is derived from the GDPR). For consent to be valid, it must be informed, specific, freely given and must constitute a real and unambiguous indication of the individual’s wishes (which has been interpreted by the Court of Justice of the EU as requiring a “clear affirmative action”). This does not apply if the cookie or similar technology: (i) is for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or (ii) is strictly necessary to provide an ISS (e.g., a service over the internet) requested by the subscriber or user, which means that it must be essential to fulfil their request. The ICO stated in its Children’s Code that cookies placed for the sole purpose of age verification are considered to be “essential”, and therefore do not require consent.

The proposed DUA Bill proposes to reform the current cookie-related rules under the PECR, by doing away with the need to obtain opt-in consent for cookies that collect information for statistical purposes, or that enhance the appearance or functionality of a website, or allow a website’s appearance or functionality to adapt to user preferences (subject to certain conditions being met).

11.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

As noted above, under the PECR, no consent is required if the sole purpose of the cookie is carrying out the transmission of a communication or if it is strictly necessary to provide an ISS requested by the user.

11.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

One of the ICO’s strategic goals for 2025 is “go further and faster to give people meaningful control over how they are tracked online”, and the ICO has been reviewing the UK’s top 200 websites for compliant tracking practices. According to its 2025 “Online Tracking Strategy”, the ICO aims to extend the scope of its review to the top 1,000 most popular websites in the UK. The ICO has also taken enforcement action where it considers that companies have been “unlawfully processing people’s data through advertising cookies without their consent”.

11.4 What are the maximum penalties for breaches of applicable cookie restrictions?

The maximum penalty is currently £500,000. The ICO has indicated that it will largely continue to follow its established procedure of information and enforcement notices, with fines issued only in the most serious cases.

If the DUA Bill (discussed in question 20.2) is finalised in its current form, the maximum penalty for breaches of cookie restrictions under the PECR will go up to £17.5 million or 4% of annual turnover (whichever is higher), so as to align with penalties under the UK GDPR.

12 Restrictions on International Data Transfers

12.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Transfers of personal data to recipients outside of the UK can only take place if: (i) the transfer is to an “Adequate Jurisdiction” (as specified in the DPA 18 or as further specified by the ICO); (ii) the transferor has implemented one of the required safeguards as specified by the UK GDPR; or (iii) one of the derogations specified in the UK GDPR applies to the relevant transfer. The EDPB Guidelines (2/2018) set out that a “layered approach” should be taken with respect to these transfer mechanisms. This guidance is likely to remain persuasive following the UK’s departure from the EU. If the transfer is not to an Adequate Jurisdiction, the data exporter should first explore the possibility of implementing one of the safeguards provided for in the UK GDPR before relying on a derogation.

To date, the UK has issued adequacy regulations in respect of each of the EEA countries and their institutions, the jurisdictions that were considered “adequate” for the purposes of the (EU) GDPR by the European Commission as of 31 December 2020, Gibraltar, South Korea, and to a partial extent, in respect of Canada, Japan and the United States.

Following the Brexit Transition Period, the UK became a third country for the purposes of EU law. On 28 June 2021, the European Commission adopted two adequacy decisions in relation to the UK, one in relation to the GDPR (which considered, among other things, the UK’s general data protection framework and the level of access that the UK Government has to personal data for law enforcement and national security purposes) and one in relation to the Law Enforcement Directive (which assessed a number of topics including the UK’s standards regarding police and judicial cooperation in criminal matters). Following the European Commission’s adoption of these decisions, it became lawful to transfer personal data from the EEA to the UK without the need for additional protections.

Following the adoption of these decisions, the UK has joined the short list of non-EEA countries to which EEA personal data may flow without restriction. Currently this list includes Andorra, Argentina, Canada (commercial organisations), the Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, South Korea, Switzerland, the United Kingdom, the United States (commercial organisations participating in the EU–US Data Privacy Framework), and Uruguay.

The European Commission’s adequacy decisions in respect of the UK are valid until June 2025, which the European Commission is currently proposing to extend to December

2025, after which the adequacy decisions may be renewed if the UK's data protection regime continues to be deemed adequate. However, adequacy decisions can be revoked. See the example discussed in question 12.2.

12.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

When transferring personal data to a country other than an Adequate Jurisdiction, businesses must ensure that there are appropriate safeguards on the data transfer, as prescribed by the UK GDPR. The UK GDPR offers a number of ways to ensure compliance for international data transfers, of which one is consent of the relevant data subject. Other common options are the use of Standard Contractual Clauses ("SCCs") or Binding Corporate Rules ("BCRs").

In June 2021, the European Commission published a revised set of SCCs (the "New SCCs"). These revised SCCs replaced the 2001 and 2004 controller-to-controller versions, and the 2010 controller-to-processor version (the "Old SCCs"), previously maintained by the European Commission and used by data exporters to protect international transfers of personal data. However, due to Brexit, the New SCCs are not valid for restricted transfers of personal data under the UK GDPR. On 21 March 2022, the ICO introduced equivalent revised mechanisms: (i) a new UK International Data Transfer Agreement (the "IDTA"); and (ii) a UK-specific Addendum to the New SCCs, which modifies the New SCCs so that they can be used for the purposes of transfers of personal data out of the UK (the "Addendum").

The IDTA is the UK's equivalent to the New SCCs and is designed to facilitate restricted transfers of personal data under the UK GDPR between controllers, processors, sub-processors and third parties (as appropriate). The Addendum revises certain provisions of the New SCCs, when they are used in the context of transfers of personal data out of the UK.

International data transfers may also take place on the basis of contracts agreed between the data exporter and data importer provided that they conform to the protections outlined in the UK GDPR, and they have prior approval by the ICO.

International data transfers within a group of businesses can be safeguarded by the implementation of BCRs. The BCRs will always need approval from the ICO. Most importantly, the BCRs will need to include a mechanism to ensure they are legally binding and enforced by every member in the group of businesses. Among other things, the BCRs must set out the group structure of the businesses, the proposed data transfers and their purpose, the rights of data subjects, the mechanisms that will be implemented to ensure compliance with the UK GDPR and the relevant complainant procedures.

The Court of Justice of the EU in *Schrems II* (Case C-311/18) effectively invalidated the then prevalent EU-US Privacy Shield Framework. In October 2023, the UK brought into force its extension to the EU-US Data Privacy Framework (the "UK Extension"), to allow organisations in the UK to transfer personal data to US entities that are certified under the UK Extension, without the need for any other safeguards provided for under Chapter V of the UK GDPR.

12.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

International transfers of personal data will require prior approval from the ICO unless a UK GDPR-compliant mechanism has been implemented. Some of those transfer mechanisms (e.g., BCRs) require approval from the ICO in any event.

12.4 Do transfers of personal data to other jurisdictions require a transfer impact assessment? If conducting a transfer impact assessment is only mandatory in some circumstances, please identify those circumstances.

The ICO requires entities to implement a transfer risk assessment prior to transferring personal data to a jurisdiction that is not the subject of an adequacy regulation in the UK. As part of such an assessment, the data exporter must analyse whether the protection afforded to the transferred personal data by the laws of the relevant third country needs to be supplemented by additional measures to ensure a level of protection that is at least equivalent to that within the UK. The ICO has published a template transfer risk assessment tool that organisations may use for this purpose.

12.5 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?

The EDPB has issued Recommendations 01/2020 on supplementary protections to be implemented where appropriate, in respect of transfers made under SCCs, in light of the *Schrems II* decision.

In *Schrems II*, the court held that organisations could continue to rely upon SCCs to transfer EU personal data to third countries, so long as "supplementary measures" are established in order to ensure adequate levels of protection for transferred personal data.

The EDPB's Recommendations set out what these "supplementary measures" could be in practice. These include technical, contractual and organisational measures.

While the ICO is no longer bound to follow the guidance of the EDPB, its recommendations are likely to remain persuasive in the UK.

12.6 What guidance (if any) has/have the data protection authority(ies) issued in relation to the use of standard contractual/model clauses as a mechanism for international data transfers?

The European Commission's revised SCCs published on 4 June 2021 are not valid for restricted transfers of personal data under the UK GDPR. See the discussion at question 12.2 regarding the mechanisms available to UK transferors of personal data. The ICO is expected to issue further guidance in relation to the UK IDTA and Addendum, respectively.

13 Whistle-blower Hotlines

13.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

Internal whistle-blowing schemes are generally established in pursuance of a concern to implement proper corporate governance principles in the daily functioning of businesses. Whistle-blowing is designed as an additional mechanism for employees to report misconduct internally through a specific channel and supplements a business's regular information and reporting channels, such as employee representatives, line management, quality-control personnel or internal auditors who are employed precisely to report such misconduct.

The WP29 has limited its Opinion 1/2006 on the application of EU data protection rules to internal whistle-blowing schemes to the fields of accounting, internal accounting controls, auditing matters, the fight against bribery, banking and financial crime. The scope of corporate whistle-blower hotlines, however, does not need to be limited to any particular issues. In the Opinion, it is recommended that the business responsible for the whistle-blowing scheme should carefully assess whether it might be appropriate to limit the number of persons eligible for reporting alleged misconduct through the whistle-blowing scheme, and whether it might be appropriate to limit the number of persons who may be reported through the scheme; in particular, in the light of the seriousness of the alleged offences reported. This guidance likely remains persuasive following the UK's departure from the EU.

13.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous reporting is not prohibited under UK data protection law; however, it raises problems as regards the essential requirement that personal data should only be collected fairly. In Opinion 1/2006, the WP29 considered that only identified reports should be advertised in order to satisfy this requirement. This guidance likely remains persuasive following the UK's departure from the EU. Businesses should not encourage or advertise the fact that anonymous reports may be made through a whistle-blower scheme.

An individual who intends to report to a whistle-blowing system should be aware that he/she will not suffer due to his/her action. The whistle-blower, at the time of establishing the first contact with the scheme, should be informed that his/her identity will be kept confidential at all the stages of the process, and in particular will not be disclosed to third parties, such as the incriminated person or the employee's line management. If, despite this information, the person reporting to the scheme still wants to remain anonymous, the report will be accepted into the scheme. Whistle-blowers should be informed that their identity may need to be disclosed to the relevant people involved in any further investigation or subsequent judicial proceedings instigated as a result of any enquiry conducted by the whistle-blowing scheme.

14 CCTV

14.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

A DPIA must be undertaken (with the assistance from the Data Protection Officer) when there is systematic monitoring of a publicly accessible area on a large scale. If the DPIA suggests that the processing would result in a high risk to the rights and freedoms of individuals prior to any action being taken by the controller, the controller must consult the ICO.

During the course of a consultation, the controller must provide information on the responsibilities of the controller and/or processors involved, the purpose of the intended processing, a copy of the DPIA, the safeguards provided by the UK GDPR to protect the rights and freedoms of data subjects and, where applicable, the contact details of the Data Protection Officer.

If the ICO is of the opinion that the CCTV monitoring would infringe the UK GDPR, it has to provide written advice to the controller within eight weeks of the request of a consultation and can use any of its wider investigative, advisory and corrective powers outlined in the UK GDPR.

14.2 Are there limits on the purposes for which CCTV data may be used?

Personal data must be collected only for specified and legitimate purposes and must be used only in a manner which is not incompatible with the original purpose. For example, if a CCTV camera is used for the purpose of monitoring criminal activity in an office, it cannot later be used for a new and fundamentally different purpose (e.g., monitoring the work attendance of employees) without the provision of fresh notice to the affected individuals informing them of the different purpose, and, where appropriate, the obtaining of consent in advance.

15 Employee Monitoring

15.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Employee monitoring must be lawful and fair. Employers must consider whether the monitoring methods are too intrusive, such that the employer's legitimate interest is outweighed by the right to privacy. Employees must be notified of the extent of the monitoring prior to commencement, and why it is taking place.

15.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

The UK GDPR requires a lawful basis for the monitoring of employees (e.g., consent or legitimate interests). However, consent is rarely used as it could easily be withheld or withdrawn by employees. In addition, because of the imbalance of power in the relationship between employer and employee, consent given in an employment context is unlikely to be deemed "freely given", and therefore would not be valid.

Generally, employers rely on the lawful basis of legitimate interests. This is subject to an assessment of proportionality and necessity. Employees must be given notice of the monitoring activities.

15.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

As good practice, trade unions and employee representatives should be consulted where applicable.

15.4 Are employers entitled to process information on an employee’s attendance in office (e.g., to monitor compliance with any internal return-to-office policies)?

Acknowledging the rise of remote working and developments in the technology available, and the increasing monitoring of employees by employers in that regard, in October 2023, the ICO published guidance on the lawful monitoring of employees in the workplace.

The guidance clarifies that prior to undertaking any employee monitoring (including monitoring for the purposes of tracking employee attendance), employers are required to comply with all applicable data protection rules, including: (i) ensuring that the employees are aware of the nature, extent and purpose of the monitoring; (ii) having a clearly defined purpose for such monitoring, and using the least intrusive means to achieve it; (iii) having a lawful basis for such processing; (iv) processing only the minimum personal data required to achieve the identified purpose; (v) implementing a DPIA for any monitoring that is likely to result in a high risk to the rights of the employees (e.g., where biometric data is involved); (vi) making the personal data collected via such monitoring available to affected employees in response to their access request; and (vii) ensuring that the personal data collected via such monitoring is accurate, secure and retained for no longer than is necessary.

16 Data Security and Data Breach

16.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Yes. Personal data must be processed in a way which ensures security and safeguards against unauthorised or unlawful processing, accidental loss, destruction and damage of the data.

Both controllers and processors must ensure they have appropriate technical and organisational measures to meet the requirements of the UK GDPR. Depending on the security risk, this may include the encryption of personal data, the ability to ensure the ongoing confidentiality, integrity and resilience of processing systems, an ability to restore access to data following a technical or physical incident, and a process for regularly testing and evaluating the technical and organisational measures for ensuring the security of processing.

16.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe.

If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

The controller is responsible for reporting a personal data breach without undue delay (and in any case within 72 hours of first becoming aware of the breach) to the ICO, unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject(s). A processor must notify any data breach to the controller without undue delay.

The notification must include the nature of the personal data breach, including the categories and number of data subjects concerned, the name and contact details of the Data Protection Officer or relevant point of contact, the likely consequences of the breach and the measures taken to address the breach, including attempts to mitigate possible adverse effects.

16.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Controllers have a legal requirement to communicate the breach to the data subject, without undue delay, if the breach is likely to result in a high risk to the rights and freedoms of the data subject.

The notification must include the name and contact details of the Data Protection Officer (or point of contact), the likely consequences of the breach and any measures taken to remedy or mitigate the breach.

The controller may be exempt from notifying the data subject if the risk of harm is remote (e.g., because the affected data is encrypted), the controller has taken measures to minimise the risk of harm (e.g., suspending affected accounts) or the notification requires a disproportionate effort (e.g., a public notice of the breach).

16.4 What are the maximum penalties for personal data security breaches?

The maximum penalty is the higher of £17.5 million or 4% of worldwide turnover.

17 Enforcement and Sanctions

17.1 Describe the enforcement powers of the data protection authority(ies).

- (a) **Investigative powers:** The ICO has wide powers to order the controller and the processor to provide any information it requires for the performance of its tasks, to conduct investigations in the form of data protection audits, to carry out reviews on certificates issued pursuant to the UK GDPR, to notify the controller or processor of alleged infringements of the UK GDPR, to access all personal data and all information necessary for the performance of controllers’ or processors’ tasks and to access the premises of the data, including any data processing equipment.

- (b) **Corrective powers:** The ICO has a wide range of powers, including the ability to issue warnings or reprimands for non-compliance, to order the controller to disclose a personal data breach to the data subject, to impose a permanent or temporary ban on processing, to withdraw a certification and to impose an administrative fine (as below).
- (c) **Authorisation and advisory powers:** The ICO has a wide range of powers to advise the controller, accredit certification bodies and to authorise certificates, contractual clauses, administrative arrangements and BCRs as outlined in the UK GDPR.
- (d) **Imposition of administrative fines for infringements of specified legal provisions:** The UK GDPR provides for administrative fines of up to the greater of £17.5 million or 4% of the business's worldwide annual turnover during the preceding financial year.
- (e) **Non-cooperation with a data protection authority:** The UK GDPR provides for administrative fines of up to the greater of £17.5 million or 4% of the business's worldwide annual turnover during the preceding financial year.

17.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The UK GDPR entitles the ICO to impose a temporary or definitive limitation, including a ban on processing.

17.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

The ICO tends to engage with businesses before it takes formal enforcement action.

17.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

The UK GDPR can also apply to non-UK businesses even if they have no physical presence in the UK (see the answer to question 3.1 above). Such businesses must appoint a representative in the UK against which the ICO can take relevant enforcement action under the UK GDPR.

18 E-discovery/Disclosure to Foreign Law Enforcement Agencies

18.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Most businesses will weigh the risks presented by non-compliance with the relevant foreign court order against those of non-compliance with the DPA 2018 and determine which are lower. Assuming that the business decides to disclose the requested personal data, businesses will usually seek to justify such disclosures on the basis that they are necessary for the establishment, exercise or defence of legal claims.

18.2 What guidance has/have the data protection authority(ies) issued on disclosure of personal data to foreign law enforcement or governmental bodies?

There is currently no standalone guidance from the ICO on this issue.

The ICO has adopted guidelines on the sharing of personal data with law enforcement authorities in general (without specifying whether this relates to foreign law enforcement authorities, though the guidance appears to be specific to UK law enforcement authorities under the UK GDPR/DPA 2018). This guidance emphasises the need to ensure that the requirements of the UK GDPR (such as ensuring that special categories of personal data are only disclosed in accordance with Articles 6, 9 and 10 of the UK GDPR) are met. The ICO has also made available an online toolkit for small organisations and businesses to guide their analysis of requests for disclosure of personal data from law enforcement authorities for personal data.

19 Artificial Intelligence

19.1 Are there any limitations on automated decision-making involving the processing of personal data using artificial intelligence?

Article 22(1) of the UK GDPR provides individuals the (qualified) right not to be subject to solely automated decision-making, including profiling, which produces legal effects concerning them or similarly significantly affects them. Solely automated decision-making is the making of decisions by technological means without human involvement, and may include decisions made by AI.

In practice, this means that businesses generally may not process the personal data of individuals solely using AI where such processing produces legal effects for those individuals or otherwise similarly significantly affects those individuals. Article 22(2) of the UK GDPR provides certain exceptions to this right – for example, where the relevant processing is necessary to enter into, or perform, a contract with the affected individual, or where the affected individual has provided their explicit (informed) consent to such processing. Where a business relies upon an exception provided under Article 22(2) of the UK GDPR, it must nevertheless implement suitable measures to safeguard the affected individual's rights, freedoms and legitimate interests, including providing the affected individual the opportunity to obtain human intervention, to express their opinion and to contest the decision made using AI.

19.2 What guidance (if any) has/have the data protection authority(ies) issued in relation to the processing of personal data in connection with artificial intelligence?

The ICO has published "Guidance on AI and Data Protection", which sets out best practices for the use of data protection-compliant AI and the ICO's interpretation of the key data protection principles such as transparency and fairness as they apply to personal data processed in the AI lifecycle. The ICO has also co-authored separate guidance (together with the Alan Turing Institute) on explaining AI-assisted or AI-generated decisions to individuals (which is relevant to compliance with Articles 5, 13, 14 and 22 of the UK GDPR, in particular).

The ICO has also developed an “AI and data protection risk” toolkit to help organisations assess the risks posed by the AI systems they have developed or deployed to affected individuals’ rights and freedoms.

The ICO forms part of the UK’s Digital Regulation Cooperation Forum (“DRCF”), together with the Competition and Markets Authority (“CMA”), the Office of Communications and the Financial Conduct Authority. The role of the DRCF is to provide a greater level of cooperation between regulators in light of the unique challenges posed by regulation of online platforms and digital services, including AI.

20 Trends and Developments

20.1 In your opinion, what enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.

The majority of the ICO’s enforcement action over the previous 12 months has been focused on breaches of applicable direct marketing law (under the PECR; see section 10 above for further discussion) and security-related requirements of the UK GDPR (e.g., in March 2025, the ICO issued a penalty of just over £3 million for failure by a processor to implement appropriate security measures in the context of a ransomware incident; it also issued a notice of intent to impose a fine of £4.5 million in connection with a personal data breach).

Generally, the ICO exercises its punitive enforcement powers under the UK GDPR in response to actual or potential non-compliance that the ICO considers serious or systematic. In other cases, the ICO tends to engage with organisations, providing them with an opportunity outside the formal enforcement framework to remedy non-compliance, or issue reprimands accompanied by its recommendations.

20.2 In your opinion, what “hot topics” are currently a focus for the data protection regulator?

An area of continued focus for the ICO has been the protection of the personal data of children. In particular, the AADC was published on 2 September 2020, and compliance has been required since 2 September 2021. The AADC applies to providers of online products or services (including apps, programs, websites, games or community environments, and connected toys or devices with or without a screen) that process personal data and are likely to be accessed by children in the UK. According to the AADC, its purpose is to address how to design data protection safeguards into online services to ensure that they are appropriate for use by, and meet the development needs of, children. The AADC goes on to state that businesses that fail to comply with the AADC would likely find it more difficult to demonstrate that their processing is fair and complies with the GDPR and PECR, and would therefore be more likely to face sanctions. In April 2024, the ICO published its 2024–2025 priorities for protecting children’s personal information online, seeking to mitigate “potential data harms to children” online. In April 2024, the ICO also published its detailed findings following its review of the financial services sector’s use of children’s data, which

included various recommendations concerning data protection governance, transparency, consent, data subject rights and marketing.

The ICO has demonstrated an increasing focus on the data protection concerns associated with the swift expansion of AI technologies in recent years. As noted in question 19.2 above, the ICO has published “Guidance on AI and Data Protection”, which sets out best practices for the use of data protection-compliant AI and the ICO’s interpretation of the key data protection principles such as transparency and fairness as they apply to personal data processed in the AI lifecycle. In June 2023, the ICO launched its “Innovation Advice” service designed to provide a fast, direct advisory service to organisations doing new or innovative things with personal data. In January 2024, the ICO launched a consultation series on how aspects of data protection law should apply to the development and use of generative AI models. In April 2024, the ICO published a report on its strategic approach to AI regulation, which – among other things – notes that AI and its application in biometric technologies is one of the ICO’s “three focus areas” for 2024–2025 (together with children’s privacy and online tracking). In December 2024, the ICO published its response to its consultation series on how the UK GDPR and the DPA 2018 apply to the development and use of generative AI.

Separately, after the Data Protection Bill did not proceed, in October 2024 the UK Government introduced the DUA Bill, which largely builds upon the Data Protection Bill and is set to reform UK’s legislative and regulatory regime for the use of, and access to, data. The stated core objectives of the DUA Bill are “growing the economy”, “improving UK public services” and “making people’s lives easier” through the introduction of new rules concerning “smart data” and digital verification services (among other things) and the modernisation of the UK’s existing data protection legislative and regulatory regime. For instance, the DUA Bill proposes new powers for enforcing the rules on cookies and direct marketing under the PECR. It proposes that the Information Commission (which will replace the ICO) will have the power to issue fines of up to £17.5m or 4% of annual turnover (whichever is higher) for breaches of the PECR, which is a significant increase from the current fine limit of £500,000. This change will be particularly impactful, considering direct marketing and cookie use (areas of compliance under the PECR) are also topics of regulatory focus for the ICO (see sections 10 and 11 above). The DUA Bill also proposes new rules regarding cookie consent, data subject right requests, automated decision-making and legitimate interests, among other things. At the time of writing, the DUA Bill is in its final stages, and is expected to come into force in early 2026.

The ICO has emphasised its intention to update its existing guidance on AI and data protection to take account of generative AI, and to align this with its upcoming joint statement with the CMA on AI foundation models, once the DUA Bill is finalised.

Note

This publication is provided for your convenience and does not constitute legal advice. This publication is protected by copyright.



Tim Hickman is a partner in the London office of White & Case and is head of the Firm's Data, Privacy & Cybersecurity practice. He advises on all aspects of data protection law and artificial intelligence (AI) regulation. Tim has significant experience of working with a wide range of clients in the UK, EU, Asia and the US.

"Working with Tim Hickman has been a pleasure, I'm continually impressed with his depth of knowledge and experience in handling complicated privacy compliance issues. One of the most significant advantages of working with Tim is his ability to coordinate efficiently with other countries' colleagues at W&C to deliver what we ask in a cost-effective approach." – *The Legal 500*, UK 2025.

White & Case LLP

5 Old Broad Street
London, EC2N 1DW
United Kingdom

Tel: +44 20 7532 2517

Email: tim.hickman@whitecase.com

LinkedIn: www.linkedin.com/in/tim-hickman-64483b77



Aishwarya Jha is an associate in the London office of White & Case. She qualified as a solicitor in the Republic of Ireland in 2021, and currently practises in England & Wales. Aishwarya has meaningful experience of working with clients in the EU, UK and US on a wide range of privacy, cybersecurity and AI matters. She has undertaken legal secondments at the Irish Data Protection Commission (in 2021) and Meta (in 2023–24), and has practical insight into the regulatory regimes for data protection in the United Kingdom, the Republic of Ireland, and Nigeria.

White & Case LLP

5 Old Broad Street
London, EC2N 1DW
United Kingdom

Tel: +44 20 7532 1230

Email: aishwarya.jha@whitecase.com

LinkedIn: www.linkedin.com/in/aishjha

With one of the largest and most experienced data privacy, artificial intelligence, and cybersecurity groups in the world, White & Case's global team is on hand to guide clients through the relevant data protection legislation in the jurisdictions in which they are active. Seamlessly working with their counterparts in other practice areas, our global team has the depth of resources to provide integrated, creative and practical advice on the privacy-related concerns faced by our clients, wherever they are located.

Our experience spans the full range of industry sectors, including financial institutions and banking, biotechnology, pharmaceuticals and chemicals, construction and engineering, consumer goods and retail, automotive, hotels and leisure, IT, telecommunications, internet and social media, artificial intelligence, manufacturing and electronics, and publishing and media.

www.whitecase.com

WHITE & CASE

USA

White & Case LLP



F. Paul Pittman



Abdul Hafiz



Andrew Hamm

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

There is no single principal data protection legislation in the United States (U.S.). Rather, a patchwork of hundreds of laws enacted on both the federal and state levels serve to protect the personal data of U.S. residents. At the federal level, the Federal Trade Commission Act (FTC Act) (15 U.S. Code § 41 *et seq.*) broadly empowers the U.S. Federal Trade Commission (FTC) to bring enforcement actions to protect consumers against unfair or deceptive practices and to enforce federal privacy and data protection regulations. The FTC has taken the position that “deceptive practices” include a company’s failure to comply with its published privacy promises or use of deceptive advertising or marketing methods and that “unfair practices” include its failure to provide adequate security of personal information.

As described more fully below, other federal statutes primarily address specific sectors, such as financial services, children or healthcare. In parallel to the federal regime, state-level statutes protect a wide range of privacy rights of individual residents. The protections afforded by state statutes often differ considerably from one state to another, and some are comprehensive, while others cover areas as specific and diverse as protecting library records to keeping homeowners free from drone surveillance.

1.2 Is there any other general legislation that impacts data protection?

Although there is no general federal legislation impacting data protection, there are a number of federal data protection laws that are sector-specific (see question 1.3 below), or focus on particular types of data. By way of example, the Driver’s Privacy Protection Act of 1994 (18 U.S. Code § 2721 *et seq.*) governs the privacy and disclosure of personal information gathered by state Departments of Motor Vehicles. Children’s information is protected at the federal level under the Children’s Online Privacy Protection Act (COPPA) (15 U.S. Code § 6501), which prohibits the collection of any information from a child under the age of 13 online and from digitally connected devices, and requires publication of privacy notices and collection of verifiable parental consent when information from children is being collected. The Video Privacy Protection Act (18 U.S. Code § 2710 *et seq.*) restricts the

disclosure of rental or sale records of videos or similar audio-visual materials, including online streaming. Similarly, the Cable Communications Policy Act of 1984 includes provisions dedicated to the protection of subscriber privacy (47 U.S. Code § 551). Finally, even in the absence of legislation, presidential administrations are often active with rulemaking, executive orders and other authorities. For example, the Biden-Harris and Trump-Vance administrations each issued an Executive Order addressing the continuing development of artificial intelligence (AI).

State laws also may impose restrictions and obligations on businesses relating to the collection, use, disclosure, security or retention of special categories of information, such as biometric data, medical records, social security numbers, driver’s licence information, email addresses, library records, television viewing habits, financial records, tax records, insurance information, criminal justice information, phone records and education records, to name some of the most common.

Every state has adopted data breach notification legislation that applies to certain types of personal information about its residents. Even if a business does not have a physical presence in a particular state, it typically must comply with the state’s laws when faced with the unauthorised access to, or acquisition of, personal information it collects, holds, transfers or processes about that state’s residents. The types of information subject to these laws vary, with most states defining personal information in the data breach context to include an individual’s first name or first initial and last name, together with a data point including the individual’s SSN, driver’s licence or state identification card number, financial account number or payment card information.

Some states are more active than others when it comes to data protection. Massachusetts, for example, has strong data protection regulations (201 CMR 17.00), requiring any entity that receives, stores, maintains, processes or otherwise has access to “personal information” of a Massachusetts resident in connection with the provision of goods or services, or in connection with employment, (a) to implement and maintain a comprehensive written information security plan addressing 10 core standards, and (b) to establish and maintain a formal information security programme that satisfies eight core requirements, which range from encryption to information security training.

In 2019, New York expanded its data breach notification law to include the express requirement that entities develop, implement and maintain “reasonable” safeguards to protect the security, confidentiality and integrity of private information. Significantly, New York’s Stop Hacks and Improve Electronic Data Security Act (N.Y. Gen Bus. Law § 899-bb)

identified certain administrative, technical and physical safeguards which, if implemented, are deemed to satisfy New York's reasonableness standard under the law. Previously, New York prioritised the regulation of certain financial institutions doing business in the state, by setting minimum cybersecurity standards, with requirements for companies to perform periodic risk assessments and file annual compliance certifications (23 NYCRR 500). In 2023, the New York Department of Financial Services (NYDFS) adopted final amendments to its revised Cybersecurity Requirements for Financial Services Companies, which includes banks, financial services and insurance companies, among other entities. These final amendments will become fully effective by 2025.

Illinois has a uniquely expansive state law (740 ILCS 14), which imposes requirements on businesses that collect or otherwise obtain biometric information and allows private individuals to sue and recover damages for violations. In January 2019, the Illinois Supreme Court offered an expansive reading of the protections of the Illinois Biometric Privacy Act (BIPA), holding that the law does not require individuals to show they suffered harm other than a violation of their legal rights to sue. Recent decisions have continued the trend toward an expansive reading of BIPA. In February 2023, the Illinois Supreme Court held that claims brought under BIPA are subject to a five-year statute of limitations. In 2024, the Illinois legislature passed a reform such that violations are counted on a "per person", not a "per scan", basis, limiting the possible damages occurring when the same person was scanned multiple times. Multiple other states have considered similar legislation in recent years.

Washington has a comprehensive health information-related law with broad scope and application. The Washington My Health My Data Law (WMHMYDA) aims to safeguard consumer health data beyond the scope of the federal Health Insurance Portability and Accountability Act (HIPAA) by regulating the collection, sharing and selling of consumer health data by any entity that conducts business or controls or processes consumer health data, in Washington. The WMHMYDA notably provides for a private right of action for consumers to seek actual (not statutory) damages, while authorising courts to impose treble damages up to a maximum of US\$25,000.

California has a long history of adopting privacy-forward legislation, and in 2018, the state enacted the California Consumer Privacy Act (CCPA), which became effective on January 1, 2020. The law introduced new obligations on covered businesses, including requirements to disclose the categories of personal information the business collects about consumers, the specific pieces of personal information the business collected about the consumer, the categories of sources from which the personal information is collected, the business or commercial purpose for collecting or selling personal information, and the categories of third parties with which the business shares personal information. It also introduced new rights for California residents, including the right to request access to and deletion of personal information and the right to opt out of having personal information sold to third parties.

Over the past five years, almost half the states enacted similar comprehensive consumer data privacy laws. Specifically, in 2020, California amended the CCPA with the California Privacy Rights Act (CPRA), which expanded the rights granted to consumers and increased compliance obligations on businesses. In 2021, Virginia enacted the Consumer Data Protection Act (Virginia CDPA), becoming the second

state with a comprehensive data privacy law, followed shortly thereafter by Colorado, which enacted the Colorado Privacy Act. Continuing this trend, in 2022, Utah enacted the Utah Consumer Privacy Act and Connecticut enacted an Act Concerning Personal Data Privacy and Online Monitoring (Connecticut Privacy Act). In 2023, Delaware, Florida, Indiana, Iowa, Montana, Oregon, Tennessee and Texas all passed state comprehensive consumer data privacy laws, followed in 2024 by Kentucky, Maryland, Minnesota, Nebraska, New Hampshire, New Jersey and Rhode Island. In the absence of a data privacy framework at the federal level, states continue to pursue legislation. In addition, state regulators are also actively making rules to implement these laws. As of July 31, 2025, the laws from California, Colorado, Connecticut, Delaware, Florida, Iowa, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Tennessee, Texas, Utah and Virginia will all be effective, with Maryland due to become effective on October 1, 2025.

1.3 Is there any sector-specific legislation that impacts data protection?

Key sector-specific laws include those covering financial services, healthcare, telecommunications and education.

The Gramm Leach Bliley Act (GLBA) (15 U.S. Code § 6802(a) *et seq.*) governs the protection of personal information in the hands of banks, insurance companies and other companies in the financial service industry. This statute addresses "Non-Public Personal Information" (NPI), which includes any information that a financial service company collects from its customers in connection with the provision of its services. It imposes requirements on financial service industry companies for securing NPI, restricting disclosure and use of NPI and notifying customers when NPI is improperly exposed to unauthorised persons.

The Fair Credit Reporting Act (FCRA), as amended by the Fair and Accurate Credit Transactions Act (15 U.S. Code § 1681), restricts use of information with a bearing on an individual's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living to determine eligibility for credit, employment or insurance. It also requires the truncation of credit card numbers on printed receipts, requires the secure destruction of certain types of personal information, and regulates the use of certain types of information received from affiliated companies for marketing purposes.

In addition to financial industry laws and regulation, the major credit card companies require businesses that process, store or transmit payment card data to comply with the Payment Card Industry Data Security Standard.

The HIPAA, as amended (29 U.S. Code § 1181 *et seq.*) protects information held by a covered entity that concerns health status, provision of healthcare or payment for healthcare that can be linked to an individual. Its Privacy Rule regulates the collection and disclosure of such information. Its Security Rule imposes requirements for securing this data.

The Telephone Consumer Protection Act (TCPA) (47 U.S. Code § 227) and associated regulations regulate calls and text messages to mobile phones, and regulate calls to residential phones that are made for marketing purposes or using automated dialling systems or pre-recorded messages. Relatedly, the Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act) (15 U.S. Code § 7701 *et seq.*) and associated regulations set basic rules for sending commercial emails, including providing an opt-out right to recipients.

The Family Educational Rights and Privacy Act (20 U.S.C. § 1232g) provides students with the right to inspect and revise their student records for accuracy, while also prohibiting the disclosure of these records or other personal information on the student, without the student's or parent's (in some instances) consent.

Where a federal statute covers a specific topic, the federal law may pre-empt any similar state law on that topic. However, certain federal laws, like the GLBA for instance, specify that they are not pre-emptive of state laws on the subject.

1.4 What authority(ies) are responsible for data protection?

While the U.S. has no plenary data protection regulator, the FTC's authority is very broad, and often sets the tone on federal privacy and data security issues. In addition, a variety of other agencies regulate data protection through sectoral laws, including the Office of the Comptroller of the Currency, the Department of Health and Human Services (HHS), the Federal Communications Commission (FCC), the Securities and Exchange Commission (SEC), the Consumer Financial Protection Bureau (CFPB) and the Department of Commerce. At the state level, the CPRA established the first dedicated privacy regulator in the U.S., the California Privacy Protection Agency (CPPA). The CPPA's responsibilities include enforcement of the CPRA with the California Attorney General, rule-making under the CPRA, and promoting public awareness of privacy issues. Other states have continued to authorise their Attorneys General to conduct rulemaking or to bring enforcement actions related to violations of their respective data privacy law.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **“Personal Data”**
In the U.S., information relating to an individual is typically referred to as “personal information” (rather than personal data), though notably, recent privacy legislation from states including Virginia, Colorado, Utah and Connecticut use the term “personal data”. The definition of personal information in the U.S. is not uniform across all states or all regulations. In addition, certain data may be considered personal information for one purpose but not for another.
- **“Processing”**
The definition of processing in the U.S. is not uniform across all states or all regulations. The general concept encompasses any operations performed on personal information or data, including collection, use, storage, disclosure, transfer, analysis, etc.
- **“Controller”**
Unlike California, more recent states, including in Virginia, Colorado, Utah and Connecticut, have incorporated this term in their data privacy legislation. Though definitions may vary, the general concept refers to the entity that determines the purpose and means of processing personal information.
- **“Processor”**
Unlike California, more recent states, including in Virginia, Colorado, Utah and Connecticut, have

incorporated this term in their data privacy legislation. Though definitions may vary, the general concept refers to an entity that processes personal information on behalf of a controller.

- **“Data Subject”**
The state data protection statutes typically cover a “consumer” residing within the state. The definition of “consumer” differs by state. Under most state data protection statutes, a “consumer” is an individual resident of the state and who engages with a business for personal, family or household purposes. In contrast, under the CCPA, a “consumer” is defined broadly as a “natural person who is a California resident”.
- **“Sensitive Personal Data”/“Special Categories of Personal Data”**
The definition of processing in the U.S. is not uniform across all states or all regulations. For those jurisdictions that consider sensitive personal data, it refers to personal information of heightened concerns, potentially including racial or ethnic origin, genetic or biometric data, citizenship, sexual orientation, health information, information in children, online browsing data or precise geolocation data.
- **“Data Breach”**
The definition of a data breach depends on the individual state statute, but typically involves the unauthorised access or acquisition of computerised data that compromises the security, confidentiality or integrity of personal information.
- **“Profiling”**
The definition of profiling depends on the individual state statute, but typically involves automated processing, potentially with human oversight, performed on personal data to evaluate, analyse or predict various aspects of identified or identifiable natural person's characteristics, potentially including economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

3 Territorial and Material Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

Businesses established in other jurisdictions may be subject to both federal and state data protection laws for activities impacting U.S. residents whose information the business collects, holds, transmits, processes or shares.

3.2 Do the data protection laws in your jurisdiction carve out certain processing activities from their material scope?

State comprehensive data privacy laws generally set thresholds (such as gross revenue from the sale of personal data or the number of consumers whose data is controlled or processed) under which all processing activities are carved out from the laws' requirements. Additionally, many exempt processing from several categories of entities covered by other laws, including state and city government agencies, certain financial institutions, non-profit organisations and institutions of higher education, though these entities' processing activities may be governed by other sector-specific federal or state data protection laws.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
The FTC has issued guidelines espousing the principle of transparency, recommending that businesses: (i) provide clearer, shorter and more standardised privacy notices that enable consumers to better comprehend privacy practices; (ii) provide reasonable access to the consumer data they maintain that is proportionate to the sensitivity of the data and the nature of its use; and (iii) expand efforts to educate consumers about commercial data privacy practices.
- **Lawful basis for processing**
While there is no “lawful basis for processing” requirement under U.S. law, the FTC recommends that businesses provide notice to consumers of their data collection, use and sharing practices and obtain consent in limited circumstances where the use of consumer data is materially different than claimed when the data was collected, or where sensitive data is collected for certain purposes. Certain new state laws require obtaining consent in certain circumstances, such as prior to processing sensitive personal data.
- **Purpose limitation**
The FTC recommends privacy-by-design practices that include limiting “data collection to that which is consistent with the context of a particular transaction or the consumer’s relationship with the business, or as required or specifically authorized by law”.
- **Data minimisation**
See above. In addition, the CCPA issued guidance noting that data minimisation is a foundational principle in the CCPA that applies to each purpose for which a business collects, uses, retains and shares personal information, and the processing of consumer’s CCPA requests.
- **Proportionality**
See above.
- **Retention**
The FTC recommends privacy-by-design practices that implement “reasonable restrictions on the retention of data”, including disposal “once the data has outlived the legitimate purpose for which it was collected”. Additionally, state laws may also specify specific retention parameters. For example, Texas’s Capture or Use of Biometric Identifier Act requires the destruction of biometric identifiers within a reasonable time, but not more than a year after the purpose for capturing the biometric identifiers has ended.
- **Accuracy**
The FTC has enforced the FTC Act against data brokers making false claims about the accuracy of their data, such as on a credit report, and businesses that inaccurately describe their collection and processing of personal data. State comprehensive data privacy laws offer consumers the right to correct inaccuracies in their personal data.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to (copies of) data/information about processing**
These rights are statute-specific. For example, under

certain circumstances, employees are entitled to receive copies of data held by employers. In other circumstances, parents are entitled to receive copies of information collected online from their children under the age of 13. Under the HIPAA, individuals are entitled to request copies of medical information held by a health services provider. At the state level, the CCPA provides a right of access to California residents for personal information held by a business relating to that resident. Other state privacy laws, including the Virginia CDPA, Colorado Privacy Act, Utah Consumer Privacy Act and the Connecticut Privacy Act, provide a similar right.

- **Right to rectification of errors**
These rights are statute-specific. Some laws, such as the FCRA, provide consumers with a right to review data about the consumer held by an entity and request corrections to errors in that data. At the state level, the right to correct information commonly attaches to credit reports, as well as criminal justice information, employment records and medical records. State data privacy legislation, including the CCPA, Virginia CDPA, Colorado Privacy Act and the Connecticut Privacy Act, provide a consumer the right to correct inaccuracies in personal data held by a business.
- **Right to deletion/right to be forgotten**
These rights are statute-specific. By way of a federal law example, the COPPA provides parents the right to review and delete their children’s information and may require that data be deleted even in the absence of a request. Some state laws, such as the CCPA, provide a right of deletion for residents of the respective states, with certain exceptions. Recent state privacy laws, including the CPRA, Virginia CDPA, Colorado Privacy Act, Utah Consumer Privacy Act and the Connecticut Privacy Act, provide a similar right to delete.
- **Right to object to processing**
These rights are statute-specific. Individuals are given the right to opt out of receiving commercial (advertising) emails under the CAN-SPAM Act and the right to not receive certain types of calls to residential or mobile telephone numbers without express consent under the TCPA. Some states provide individuals with the right not to have telephone calls recorded without either consent of all parties to the call or consent of one party to the call. Under the CCPA, consumers have the right to opt out of the sale of personal information and the processing of sensitive information (in certain circumstances).
- **Right to restrict processing**
These rights are statute-specific. Certain laws restrict how an entity may process consumer data. For example, the CCPA allows California residents, and the Nevada Privacy Law allows Nevada residents, to prohibit a business from selling that individual’s personal information. Recent state privacy laws, including the Virginia CDPA, Colorado Privacy Act and Connecticut Privacy Act, provide a right to restrict processing for the purposes of sale, targeted advertising and profiling. The CCPA allows consumers to opt out of the processing of sensitive personal information except for certain specific purposes. The Utah Consumer Privacy Act provides a slightly narrower right to restrict processing for the purposes of sale or targeted advertising.
- **Right to data portability**
These rights are statute-specific. Examples of consumer rights to data portability exist under the HIPAA, where individuals are entitled to request that medical

information held by a health services provider be transferred to another health services provider. In addition, state privacy laws, including the CCPA, Virginia CDPA, Colorado Privacy Act, Utah Consumer Privacy Act and the Connecticut Privacy Act, provide a right to data portability.

- **Right to withdraw consent**
These rights are statute-specific. By way of example, under the TCPA, individuals are permitted to withdraw consent required to permit a business to send certain types of calls or texts to residential or mobile telephone lines. For an example under state law, the Colorado Privacy Act requires that consumers have the right to withdraw consent, because the regulations do not consider consent that a consumer cannot easily withdraw, to “be freely given”. Other state laws, such as the CCPA, address the right to withdraw consent by empowering users to limit the processing of sensitive personal data at any time.
- **Right to object to marketing**
These rights are statute-specific. Several laws permit consumers to restrict marketing activities involving their personal data. Under the CAN-SPAM Act, for example, individuals may opt out of receiving commercial (advertising) emails. Under the TCPA, individuals must provide express written consent to receive marketing calls/texts to mobile telephone lines. California’s Shine the Light Act requires companies that share personal information for the recipient’s direct marketing purposes to either provide an opt-out or make certain disclosures to the consumer of what information is shared, and with whom. State privacy laws, including the CCPA, Virginia CDPA, Colorado Privacy Act, Utah Consumer Privacy Act and the Connecticut Privacy Act, provide consumers with the right to opt out of processing of their personal information for targeted advertising.
- **Right protecting against solely automated decision-making and profiling**
State privacy rules against profiling, including in California, Virginia, Colorado and Connecticut, became effective for the first time in 2023.
- **Right to complain to the relevant data protection authority(ies)**
These rights are statute-specific. By way of example, individuals may report unwanted or deceptive commercial email (“spam”) directly to the FTC, and telemarketing violations directly to the FCC. Similarly, anyone may file a HIPAA complaint directly with the HHS. At the state level, California residents may report alleged violations of the CCPA to the California Attorney General or the CPPA. Similarly, the Utah Consumer Privacy Act provides that Utah residents may report alleged violations to the state’s Consumer Protection Division.

5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

This is not applicable in our jurisdiction. A few U.S. data privacy laws allow for individuals to institute an action for violations of data privacy statutes or regulations, including actions that could take the form of a class action or collective redress. However, most U.S. data privacy laws do not authorise such individual actions. Rather, the trend under U.S. data privacy laws is to restrict enforcement to regulators.

6 Children’s Personal Data

6.1 What additional obligations apply to the processing of children’s personal data?

Children’s information is protected at the federal level under the COPPA (15 U.S. Code § 6501). The COPPA requires operators of: (a) commercial websites and online services directed to children under the age of 13; or (b) general or mixed audience commercial websites or online services with actual knowledge they are collecting personal information from children under the age of 13 to meet specific compliance obligations where they collect personal information from children under the age of 13. Specifically, the COPPA requires that covered operators: (1) publish certain privacy notices, including a COPPA-compliant privacy policy and “direct notice” to parents prior to the collection of personal information from their child; (2) obtain parental consent prior to collecting personal information from a child under the age of 13; (3) provide parents a choice regarding disclosure of a child’s information to third parties under certain circumstances; (4) provide parents access to their child’s personal information and opportunities to delete that information or prevent further use or collection of a child’s information; and (5) maintain the confidentiality, security and integrity of the information collected.

At the state level, the CCPA alters its right to opt out of sale of personal information for consumers under the age of 16. Businesses are prohibited from selling personal information of consumers under the age of 16 without affirmative authorisation from a consumer aged 13–15 or from the parent or legal guardian of a consumer under the age of 13. Recent privacy laws, including in Virginia, Colorado, Utah and Connecticut, consider the personal data of a child below the age of 13 as sensitive personal data. In Virginia, Utah and Connecticut, controllers must process a child’s data in accordance with the COPPA. The Colorado Privacy Act requires consumer consent before processing sensitive personal data, but notably exempts personal data subject to the COPPA. In 2022, California enacted the Age-Appropriate Design Code Act, which imposes requirements addressing transparency requirements, default settings and data protection impact assessments. Notably, the law, effective July 1, 2024, applies to children under 18, not under 13 like the COPPA or other laws involving children’s data.

7 Registration Formalities and Prior Approval

7.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

Vermont, California, Texas and Oregon require data brokers to register, with the respective Attorneys General (Vermont and California), Secretary of State (Texas), or Department of Consumer and Business Services (Oregon). The Vermont requirement defines a “data broker” to include entities that knowingly collect and sell or license to third parties the personal information of a consumer with whom the business does not have a direct relationship (9 V.S.A. chapter 62). California’s data broker definition similarly encompasses the knowing collection and sale of personal information regarding consumers with which the business does not have a direct relationship (Cal. Civ. Code § 1798.99.80(d)). Texas defines “data broker” as “a business entity whose principal source of

revenue is derived from the collecting, processing, or transferring of *personal data* that the entity did not collect directly from the individual linked or linkable to the data” (Tex. Bus. & Com. Code Ann. § 509.001(4)). In Oregon, a “data broker” is a “business entity or part of a business entity that collects and sells or licenses brokered personal data to another person” (Or. Rev. Stat. § 646A.593(1)(c)(A)).

7.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

The states that have mandated data broker registration generally do not require a specific description of relevant data processing activities. California makes it optional for the data broker to provide within its registration any information concerning its data collection practices (Cal. Civ. Code § 1798.99.82). Vermont, in contrast, is more demanding and requires registrants to disclose information regarding consumer opt-out, whether the data broker implements a purchaser credentialing process, and the number and extent of any data broker security breaches it experienced during the prior year. Where data brokers knowingly possess information about minors, Vermont law requires that they detail all related data collection practices, databases, sales activities and opt-out policies (9 V.S.A. § 2446). Texas’s law is similar to Virginia’s, though it only requires information regarding opt-outs that are applicable to the personal data of a known child (Tex. Bus. & Com. Code Ann. § 509.005(b)(5)(A)). Oregon requires a description of the methods that consumers can use to opt out of the collection, selling and licensing of personal data (Or. Rev. Stat. § 646A.593(3)(c)).

7.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

Data broker registrations are made on a “per legal entity” basis.

7.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

Within the states for which it applies, registrations are required based on the business falling within the definition of a “data broker” pursuant to state law. Generally, a “data broker” is defined as a business that knowingly collects and sells the personal information of a consumer with whom the business does not have a direct relationship.

7.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

See question 7.2 above.

7.6 What are the sanctions for failure to register/notify where required?

The states impose civil penalties in addition to requiring unpaid registration fees. In Vermont, the penalty is US\$50 per day in addition to any unpaid registration fees of US\$100. In California, a data broker that fails to register is liable for civil penalties, fees and costs of US\$200 for each day the data broker fails to register and an amount equal to the fees that were due during the period it failed to register. In Texas, the civil penalty is US\$100 per day plus unpaid registration fees. In Oregon, the civil penalty is US\$500 per day plus unpaid registration fees. In Vermont, Texas and Oregon, US\$10,000 is the maximum amount of penalty and fees an entity may face per year.

7.7 What is the fee per registration/notification (if applicable)?

Fees vary by state. The data broker registration fee in Vermont is US\$100, in California it is US\$6,600 plus 2.99% for third-party processing fees, in Texas it is US\$300 and in Oregon it is US\$600.

7.8 How frequently must registrations/notifications be renewed (if applicable)?

In Vermont, California, Texas and Oregon, data brokers are required to register annually.

7.9 Is any prior approval required from the data protection regulator?

Data broker registration submissions require Attorney General approval in both Vermont and California, Secretary of State approval in Texas and Division of Consumer and Business Services approval in Oregon.

7.10 Can the registration/notification be completed online?

Data broker registration for Vermont, California, Texas and Oregon may be completed online.

7.11 Is there a publicly available list of completed registrations/notifications?

Vermont and California, Texas and Oregon maintain publicly available lists of registered data brokers.

7.12 How long does a typical registration/notification process take?

Vermont, California, Texas and Oregon do not publish information concerning the typical amount of time for the data broker registration process.

8 Appointment of a Data Protection Officer

8.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

Appointment of a Data Protection Officer is not required under U.S. law, but certain statutes require the appointment or designation of an individual or individuals who are charged with compliance with the privacy and data security requirements under the statute. These include the GLBA, HIPAA and the Massachusetts Data Security Regulation, for example.

8.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

Potential sanctions are statute/regulator-specific.

8.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

This is not applicable in our jurisdiction.

8.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

This is not applicable in our jurisdiction.

8.5 Please describe any specific qualifications for the Data Protection Officer required by law.

This is not applicable in our jurisdiction.

8.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

This is not applicable in our jurisdiction.

8.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

This is not applicable in our jurisdiction.

8.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

This is not applicable in our jurisdiction.

9 Appointment of Processors

9.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Under certain state laws and federal regulatory guidance, if

a business shares certain categories of personal information with a vendor, the business is required to contractually bind the vendor to reasonable security practices. The HIPAA, for example, requires the use of Business Associate Agreements for the transfer of protected health information to vendors. State laws such as the CCPA, Virginia CDPA, Colorado Privacy Act, Utah Consumer Privacy Act and the Connecticut Privacy Act require written contracts for certain entities that process personal information for the business/controller.

9.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The form of the contract typically is not specified. The HIPAA, however, is an example of a federal statute with minimum requirements for provisions that must be included within Business Associate Agreements. These agreements must include limitations on use and disclosure, and require vendors to abide by the HIPAA's Security Rule, to provide breach notification and report on unauthorised use and disclosure, to return or destroy protected data, and to make its books, records and practices available to the federal regulator. Requirements under state data privacy legislation vary by jurisdiction. Under the CCPA, the contract must restrict the service provider from retaining, using or disclosing personal information for any purpose other than performance of the services specified in the contract. Additional mandatory contract provisions on both service providers and contractors include requiring that contracts prohibit service providers from selling or sharing personal information and from retaining, using or disclosing personal information outside of the direct business relationship between the business and the service provider, allowing review or audits of service provider or contractors' data processing practices to ensure compliance and assisting businesses with complying with consumer rights requests. Additionally, state laws such as the Virginia CDPA, Colorado Privacy Act, Utah Consumer Privacy Act and the Connecticut Privacy Act each require that a contract set forth instructions for processing, including the type of data subject to processing and the nature and purpose of processing, and set specific requirements regarding engagement of subcontractors. The Colorado Privacy Act further requires that controllers and processors implement appropriate technical and organisational safeguards related to security.

10 Marketing

10.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

Prior express written consent is required under the TCPA before certain marketing texts may be sent to a mobile telephone line. Other federal statutes have opt-out rather than opt-in consent requirements. For instance, under the CAN-SPAM Act, marketing emails – or emails sent for the primary purpose of advertising or promoting a commercial product or service – may be sent to those not opting out, provided the sender is accurately identified, the subject line and text of the email are not deceptive, the email contains the name and address of the sender, the email contains a free, simple mechanism to opt out

of future emails, and the sender honours opt-outs within 10 days of receipt.

10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

The TCPA and CAN-SPAM Act apply to both business-to-consumer and business-to-business electronic direct marketing. In contrast, business-to-business telephone communications, except those intended to induce the retail sale of non-durable office or cleaning supplies, are exempt from the Telemarketing Sales Rule described in question 10.3 below.

10.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

Marketing by telephone is regulated on the national level by the Telemarketing Sales Rule, a regulation under the Telemarketing and Consumer Fraud and Abuse Prevention Act. This act established the national Do Not Call (DNC) list of telephone numbers that cannot be used for marketing communications (calls and texts) and disclosure requirements for companies engaging in telephone marketing. It also proscribes limitations on the use of telephone marketing, including, for instance, limiting the time of day for marketing calls, requiring the caller to provide an opt-out of future calls and limiting the use of pre-recorded messages. There are no consent or opt-out requirements for sending marketing materials through postal mail. In addition, with the growing prevalence of telemarketers using spoofed caller IDs, the FCC is becoming more aggressive with its enforcement of the Truth in Caller ID Act. Furthermore, several states maintain an independent DNC list and regulations in which telemarketers must comply.

It is noted that the FTC, which regulates deceptive practices, has brought enforcement actions relating to the transmission of marketing emails or telemarketing calls by companies who have made promises in their publicly posted privacy policies that personal information will not be used for marketing purposes. Additionally, many states apply deceptive practices statutes to impose penalties or injunctive relief in similar circumstances, or where violation of a federal statute is deemed a deceptive practice under state law. Finally, recent comprehensive state data privacy laws, including in California, Virginia, Colorado, Utah and Connecticut, offer consumers an opt-out of sale, disclosure or processing of personal information in relation to targeted advertising or profiling.

10.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Potentially, depending on if the entity sending the marketing is subject to jurisdiction in U.S. court and if the recipient is within the U.S.

10.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

The FTC, FCC and the Attorneys General of the states are active in enforcement in this area.

10.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Yes. However, the purchaser of the list should correlate it with the national DNC list and the purchaser's email opt-out lists. Some states forbid the sale of email addresses of individuals who have opted out of receiving marketing emails, and some forbid the sale of information obtained in connection with a consumer's purchase transaction.

10.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

The penalties under the CAN-SPAM Act can reach as high as US\$51,744 per email. The penalties under the TCPA are US\$500 per telephone call/text message violation, US\$1,500 for each willful or knowing violation and additional civil forfeiture fees with a penalty of up to US\$10,000 for intentional violations (based on the Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, passed in 2019), plus fines that can reach US\$16,000 for each political message or call sent in violation of the Act. Once a consumer's telephone number has been registered on the DNC registry for 31 days, DNC laws prohibit a business from calling it. The business can be fined up to US\$11,000 per call by the New York Department of State, as well as by the FTC and FCC. By way of example, the FTC and the attorneys general of several states obtained a judgment of US\$280 million in 2017 for a company's repeated violation (involving over 66 million calls) of the TCPA, the FTC's Telemarketing Sales Rule and state law. Similarly, in March 2021, the FCC issued a US\$225 million fine – then the largest in the history of the agency – against telemarketers based in Texas for violations of the TCPA and the Truth in Caller ID Act in connection with approximately 1 billion robocalls.

Many states have their own deceptive practices statutes, which impose additional state penalties where violations of federal statutes are deemed to be deceptive practices under the state statute.

11 Cookies

11.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

The federal Computer Fraud and Abuse Act has been used to assert legal claims against the use of cookies for behavioural advertising, where the cookies enable "deep packet" inspection of the computer on which they are placed. At least two states, California and Delaware, require disclosures to be made where cookies are used to collect information about a consumer's online activities across different websites or over time. The required disclosure must include how the operator responds to so-called "do not track" signals or other similar mechanisms. In addition, the CCPA's broad definition of "sale" (which includes when a consumer's personal information is made available for collection by third-party cookies for monetary "or other valuable consideration") and "sharing" (which encompasses the collection of data for use in cross contextual advertising), imposes obligations on businesses to provide certain notice and choice mechanisms (e.g., opt out) to consumers.

In addition, the FTC Act and state deceptive practices acts have underpinned regulatory enforcement and private class

action lawsuits against companies that failed to disclose or misrepresented their use of tracking cookies. One company settled an action in 2012 with a payment of US\$22.5 million to the FTC, and in 2016 agreed to pay US\$5.5 million to settle a private class action involving the same conduct. In 2022, one company settled with the California Attorney General for US\$1.2 million for failing to disclose to consumers that it was selling their personal information by making it available to third-party advertisers via online cookie trackers.

11.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

The Computer Fraud and Abuse Act and the Electronic Communications Privacy Act, as well as state surveillance laws, may come into play where cookies collect information from the computer on which they are placed and report that information to the entity placing the cookies without proper consent.

11.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

Yes, the FTC has brought regulatory enforcement actions against companies that failed to disclose or misrepresented their use of cookies, as well as those companies that engaged in surveillance advertising without disclosing the practice or obtaining consent (for sensitive data). The California Attorney General has also initiated regulatory investigations for violations of the CCPA rules on “selling” and “sharing” personal information that came about through the use of cookies, which in one instance, resulted in a settlement with the California Attorney General for US\$1.2 million.

11.4 What are the maximum penalties for breaches of applicable cookie restrictions?

Maximum fines are not set by statute.

12 Restrictions on International Data Transfers

12.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

The U.S. does not currently place restrictions on the transfer of personal data to other jurisdictions (however, see question 20.2 discussing the Executive Order requesting new legislation regarding bulk data transfers to “countries of concern”).

12.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

This is left to the discretion of the company, as the U.S. does not place restrictions on the transfer of personal data to other jurisdictions. With respect to receiving data from abroad, the European Commission adopted an adequacy decision for the

EU–U.S. Data Privacy Framework (DPF), providing a mechanism to comply with data protection requirements when transferring personal data from the EU to the U.S. A business may transfer data from the U.S. to the EU if the business self-certifies to the Department of Commerce that it complies with the DPF Principles. Other mechanisms to govern data transfers from the EU to the U.S. – e.g., the use of standard contractual clauses (SCCs) or binding corporate rules – remain valid.

12.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

No such registration/notification is required.

12.4 Do transfers of personal data to other jurisdictions require a transfer impact assessment? If conducting a transfer impact assessment is only mandatory in some circumstances, please identify those circumstances.

Transfers of personal data to other jurisdictions do not require a transfer impact assessment.

12.5 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?

On March 25, 2022, the U.S. and the European Commission announced that they had reached an agreement in principle to replace the Privacy Shield Framework with a new data transfer framework, the DPF. Under this framework, the U.S. has committed to strengthen privacy and civil liberties safeguards governing signals intelligence activities, establish a multi-layer redress mechanism including an independent Data Protection Review Court available to EU citizens, and enhance oversight. On October 7, 2022, President Biden signed an Executive Order, “Enhancing Safeguards for United States Signals Intelligence Activities”, intending to incorporate these commitments. In 2023, the European Commission released an adequacy decision concerning the proposed framework.

12.6 What guidance (if any) has/have the data protection authority(ies) issued in relation to the use of standard contractual/model clauses as a mechanism for international data transfers?

The FTC has expressed “commitment to vigorous enforcement” of the DPF Principles. A business need not use SCCs if the business self-certifies to the Department of Commerce that it complies with the DPF Principles.

13 Whistle-blower Hotlines

13.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

The federal Whistleblower Protection Act of 1989 protects federal employees, and some states have similar statutes

protecting state employees. Public companies subject to the Sarbanes-Oxley Act also are required to have a whistle-blower policy, which must be approved by the board of directors, and create a procedure for receiving complaints from whistle-blowers.

13.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous reporting generally is permitted. Rule 10A-3 of the Securities Exchange Act of 1934, for example, requires that audit committees of publicly listed companies establish procedures for the confidential, anonymous submission by employees of concerns regarding questionable accounting or auditing matters.

14 CCTV

14.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

The use of CCTV must comply with federal and state criminal voyeurism/eavesdropping statutes, some of which require signs to be posted where video monitoring is taking place, restrict the use of hidden cameras, or prohibit videotaping altogether if the location is inherently private (including places where individuals typically get undressed, such as bathrooms, hotel rooms and changing rooms). Litigation has been instituted alleging that CCTV may also violate biometrics laws such as the BIPA. For example, in 2024, a class of plaintiffs survived a motion to dismiss with allegations that a doorbell camera provider's cameras recording passers-by without consent violated the BIPA.

14.2 Are there limits on the purposes for which CCTV data may be used?

There generally are no restrictions on the use of lawfully collected CCTV data, subject to a company's own stated policies or labour agreements.

15 Employee Monitoring

15.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Employee privacy rights, like those of any individual, are based on the principle that an individual has an expectation of privacy unless that expectation has been diminished or eliminated by context, agreement, notice or statute. Monitoring of employees generally is permitted to the same extent as it is with the public, including when the employer makes clear disclosure regarding the type and scope of monitoring in which it engages, and subject to generally applicable surveillance laws regarding inherently private locations as well as employee-specific laws such as those regarding the privacy of union member activities.

15.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Consent and notice rights are state-specific, as is the use of hidden cameras. When required or voluntarily obtained, employers typically obtain consent for employee monitoring through acceptance of employee handbooks, and may provide notice by appropriately posting signs. Furthermore, under the CCPA, employee personal information is treated like consumer personal information under the CCPA, subject to the same consumer rights and business obligations.

15.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

The National Labor Relations Act prohibits employers from monitoring their employees while they are engaged in protected union activities.

15.4 Are employers entitled to process information on an employee's attendance in office (e.g., to monitor compliance with any internal return-to-office policies)?

Yes. As a general matter, employers are entitled to monitor employees' attendance in the office. Particular forms of monitoring could be prohibited depending on the manner and circumstances of the processing. For instance, the BIPA prohibits employers from processing employees' biometric data without consent.

16 Data Security and Data Breach

16.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

In the consumer context, the FTC has stated that a company's data security measures for protecting personal data must be "reasonable", taking into account numerous factors, to include the volume and sensitivity of information the company holds, the size and complexity of the company's operations, and the cost of the tools that are available to address vulnerabilities. Certain federal statutes and certain individual state statutes also impose an obligation to ensure security of personal information. For example, the GLBA and HIPAA impose security requirements on financial services and covered healthcare entities (and their vendors). In 2021, the FTC announced its revisions to its Safeguards Rule under the GLBA with major updates taking effect in December 2022. The updated rule requires highly prescriptive safeguards including a written incident response plan, penetration testing and vulnerability assessments, encryption of customer information and multi-factor authentication, among other safeguards. Some states impose data security obligations on certain entities that collect, hold or transmit limited types of personal information. For example, the NYDFS adopted regulations in 2017 that obligate all "regulated entities" to adopt a cybersecurity programme and cybersecurity governance processes. The regulations also mandate reporting of cybersecurity events, like data breaches and attempted infiltrations, to regulators. Covered entities include those banks, mortgage companies, insurance companies and cheque-cashers otherwise

regulated by the NYDFS. Enforcement of the NYDFS regulation began in early 2021. In 2022, the NYDFS announced a consent order against a company that was subject to four cybersecurity incidents. The company agreed to pay a US\$5 million monetary penalty, to surrender its insurance provider licences and to stop selling insurance to New York residents. In 2023, the NYDFS adopted final amendments to its Cybersecurity Requirements for Financial Services Companies, which expanded the type of activity that would be considered a violation of the Cybersecurity Requirements and imposed additional requirements relating certification, risk assessments and governance. These amendments take complete effect in 2025.

16.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

At the federal level, other than breach notification requirements pertaining to federal agencies themselves, the HIPAA requires “Covered Entities” to report impermissible uses or disclosures that compromise the security or privacy of protected health information to the HHS. Under the Privacy Rule, if the breach involves more than 500 individuals, such notification must be made within 60 days of discovery of the breach. Information to be submitted includes information about the entity suffering the breach, the nature of the breach, the timing (start and end) of the breach, the timing of discovery of the breach, the type of information exposed, safeguards in place prior to the breach and actions taken following the breach, including notifications sent to impacted individuals and remedial actions. In 2022, the U.S. enacted the Cyber Incident Reporting for Critical Infrastructure Act. Upon completion of the formal rulemaking (expected by fall 2025), this law requires companies considered part of the U.S. critical infrastructure to report substantial cybersecurity incidents to the Cybersecurity and Infrastructure Security Agency of the U.S. Department of Homeland Security within 72 hours and to report ransomware payments within 24 hours.

While not specifically a data breach notification obligation, the Securities and Exchange Act and associated regulations, including Regulation S-K, require public companies to disclose in filings with the SEC when material events, including cyber incidents, occur. To the extent cyber incidents pose a risk to a registrant’s ability to record, process, summarise and report information that is required to be disclosed in SEC filings, management should also consider whether there are any deficiencies in its disclosure controls and procedures that would render them ineffective. In 2023, the SEC adopted rules requiring disclosures regarding material cybersecurity incidents within four business days after a materiality determination, as well as specific disclosures about public companies’ cybersecurity risk management and governance in its annual disclosures.

Some state statutes require the reporting of data breaches to a state agency or Attorney General under certain conditions. The information to be submitted varies by state but generally includes a description of the incident, the number of individuals impacted, the types of information exposed, the timing of the incident and the discovery, actions taken to prevent future occurrences, copies of notices sent to impacted individuals,

and any services offered to impacted individuals, such as credit monitoring. The NYDFS also requires a Covered Entity to notify the NYDFS no later than 72 hours from a determination that a Cybersecurity Event has occurred.

16.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

At the federal level, the HIPAA requires covered entities to report data breaches to impacted individuals without unreasonable delay, and in no case later than 60 days. Notice should include a description of the breach, to include: the types of information that were involved; the steps individuals should take to protect themselves, including who they can contact at the covered entity for more information; as well as what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches. For breaches affecting more than 500 residents of a state or jurisdiction, covered entities must provide local media notice, in addition to individual notices.

As of May 2018, all 50 states, the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands have statutes that require data breaches to be reported, as defined in each statute, to impacted individuals. These statutes are triggered by the exposure of personal information of a resident of the jurisdiction, so if a breach occurs involving residents of multiple states, then multiple state laws must be followed. Most statutes define a “breach of the security of the system” as involving unencrypted computerised personal information, but some states include personal information in any format. Triggering personal information varies by statute, with most including an individual’s first name or first initial and last name, together with a data point, including the individual’s Social Security Number, driver’s licence or state identification card number, financial account number or payment card information. Some states include additional triggering data points, such as date of birth, mother’s maiden name, passport number, biometric data, employee identification number or username and password. The standard for when notification is required varies from unauthorised access to personal information, to unauthorised acquisition of personal information, to misuse of or risk of harm to personal information. Most states require notification as soon as is practical, and often within 30 to 60 days of discovery of the incident, depending on the statute. The information to be submitted varies by state but generally includes a description of the incident, the types of information exposed, the timing of the incident and its discovery, actions taken to prevent future occurrences, information about steps individuals should take to protect themselves, information resources and any services offered to impacted individuals, such as credit monitoring.

16.4 What are the maximum penalties for personal data security breaches?

Penalties are statute- and fact-specific. Under the HIPAA, for example, monetary fines can range from US\$100 to US\$50,000 per violation (or per record), with a maximum penalty of US\$1.75 million per year for each violation. By way of example, in 2020, the HHS and the Attorneys General of 42 states entered into a

US\$39.5 million settlement with a health insurer in relation to a data breach affecting the health records of over 79 million individuals. Marking the current high point for enforcement, a company agreed to pay a record penalty of at least US\$575 million, and potentially up to US\$700 million in a data breach settlement reached with the FTC, the CFPB, 48 states, the District of Columbia, and the Commonwealth of Puerto Rico.

17 Enforcement and Sanctions

17.1 Describe the enforcement powers of the data protection authority(ies).

The U.S. does not have a central data protection authority. As such, the enforcement powers of the regulators will depend on the specific statute in question. Some laws only permit federal government enforcement, some allow for federal or state government enforcement, and some allow for enforcement through a private right of action by aggrieved consumers. Whether the sanctions are civil and/or criminal depends on the relevant statute. For example, HIPAA enforcement permits the imposition of civil and criminal penalties. While the HIPAA's civil remedies are enforced at the federal level by the HHS, and at the state level by Attorneys General, the U.S. Department of Justice (DOJ) is responsible for criminal prosecutions under the HIPAA. At the state level, the CPPA has the power to enforce consumer rights and business obligations under the CPRA.

- (a) **Investigative powers:** Depending on the applicable data protection laws, regulators in the U.S. may have the authority to conduct investigations into potential violations of data protection requirements.
- (b) **Corrective powers:** Depending on the applicable data protection laws, regulators in the U.S. may have the authority to correct non-compliance actions of businesses through injunctive relief or under consent orders.
- (c) **Authorisation and advisory powers:** Depending on the applicable data protection laws, regulators in the U.S. will often provide a method for businesses to consult with the regulators for additional and specific guidance.
- (d) **Imposition of administrative fines for infringements of specified GDPR provisions:** This is not relevant for the U.S.
- (e) **Non-compliance with a data protection authority:** Depending on the applicable data protection laws, non-compliance with a data protection authority will generally attract renewed or additional enforcement against the business.

17.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The U.S. does not have a central data protection authority. Enforcement authority, including whether a regulator may ban a particular processing activity, is specified in the relevant statutes. For example, 18 states have adopted the Insurance Data Security Model Law developed by the National Association of Insurance Commissioners. Among other things, these laws empower state insurance commissioners to issue cease-and-desist orders pertaining to data processing violations in the insurance industry, and even to suspend or revoke

an insurance institution's or agent's licence to operate. The FTC may also prohibit a particular company from engaging in a particular processing activity through a negotiated consent decree as part of a settlement.

17.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

In the U.S., this depends on the relevant statutory enforcement mechanism and the agency conducting the enforcement measures. The FTC, for example, in addition to publishing on its website all of the documents filed in FTC cases and proceedings, publishes an annual summary of key data privacy and data security enforcement actions and settlements, which provides guidance to businesses on its enforcement priorities. Similarly, the HHS publishes enforcement highlights, summarises the top compliance issues alleged across all complaints and, by law, maintains a website that lists mandatorily reported breaches of unsecured protected health information affecting 500 or more individuals. By way of an example, in 2022, the FTC entered into a consent decree that required an online marketplace to destroy improperly obtained or unnecessary data, limit future data collection, and implement an information security programme. Such requirements are commonplace in FTC consent decrees.

17.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

Extraterritorial enforcement of a U.S. law would depend on a number of factors, including whether the entity is subject to the jurisdiction of the U.S. courts, the impact on U.S. commerce and the impact on U.S. residents, among other factors.

18 E-discovery/Disclosure to Foreign Law Enforcement Agencies

18.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

When made pursuant to Mutual Legal Assistance Treaties, information requests are typically processed through the DOJ, which works with the local U.S. Attorney's Office and local law enforcement, prior to review by a federal judge and service on the U.S. company. In addition, under the Clarifying Lawful Overseas User of Data Act, businesses may also receive requests for electronic communications, including personal data within its possession, custody or control directly from foreign governments and agencies that maintain agreements with the U.S., without regard to where the business stores such data.

18.2 What guidance has/have the data protection authority(ies) issued on disclosure of personal data to foreign law enforcement or governmental bodies?

This is not applicable in our jurisdiction.

19 Artificial Intelligence

19.1 Are there any limitations on automated decision-making involving the processing of personal data using artificial intelligence?

While this area is evolving in the U.S., many state data privacy laws, including the CCPA and Colorado Privacy Act, require that businesses allow users to opt out of the use of their personal data for certain profiling, including in furtherance of decisions that produce legal or other significant effects concerning a consumer. The California Privacy Protection Agency is in the process of finalising rules relating to the use of automated decision-making technology. Colorado has also promulgated the Colorado AI Act, which imposes obligations on developers and deployers to use reasonable care to protect consumers from algorithmic discrimination resulting from the use of high-risk AI systems rendering consequential decisions of material legal effect. Further, State and local laws regulating automated decision-making have been passed in Illinois and New York City. In addition, existing laws apply to automated decision-making involving the processing of personal data using AI. Section 5 of the FTC Act prohibits unfair or deceptive acts or practices, with “deceptive” acts potentially including misrepresentations in a company’s privacy policy about how users’ personal data will or will not be used as part of automated decision-making. Finally, in Executive Order 14179 on “Removing Barriers to American Leadership in Artificial Intelligence”, President Trump revoked Biden-era AI policies and directives, stating that it “is the policy of the United States to sustain and enhance America’s global AI dominance”.

19.2 What guidance (if any) has/have the data protection authority(ies) issued in relation to the processing of personal data in connection with artificial intelligence?

In 2023, the FTC stated in a blog post that “there is no AI exemption from the laws on the books”, indicating that companies utilising AI “have an obligation to abide by existing laws”. The FTC advised companies to take necessary steps to prevent harm before and after deploying a product; take preventative measures to detect, deter and halt AI-related impersonation, fraud, child sexual abuse material and non-consensual intimate imagery; avoid deceptive claims about AI tools that result in people losing money or put users at risk of harm; and ensure privacy and security by default.

20 Trends and Developments

20.1 In your opinion, what enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.

In 2024, the FTC continued its aggressive approach to enforcement with regard to data privacy and cybersecurity, with emphasis on AI, children and teens, health, geolocation and other sensitive data. In December 2024, the FTC finalised an order against a company offering AI and Deep Learning-based video analytics and video cloud software, after alleging in its complaint that the company made false, misleading or unsubstantiated representations, including about its accuracy rate, the amount of faces on which it was trained, and lack of any gender or racial bias. Nonetheless, FTC enforcement against

AI companies may decrease in the short term as the new chair of the FTC, Andrew Ferguson, has indicated less interest in regulating and controlling AI innovation.

In addition, across multiple cases, the FTC focused on failures to properly secure and use sensitive data, including enforcement actions against companies for undisclosed collection and use of consumers’ geolocation data for advertising purposes and for failure to limit advertisers’ use of shared consumer information. The FTC also filed complaints against a data broker for the allegedly unlawful selling of consumers’ precise location data.

In addition, the SEC fined the parent company of multiple stock exchanges for informing compliance and legal officials at the subsidiary exchanges only after several days. The SEC also settled with a company for its failure to establish adequate internal cybersecurity disclosure controls, delaying the company’s response to a 2021 ransomware attack. Notably, a court rejected the SEC’s argument that its authority to enforce a company’s failure to maintain adequate controls for financial reporting and asset management included authority over cybersecurity-related failures.

State Attorneys General also played a key role in the U.S. data privacy enforcement environment under specific U.S. state laws in 2024. In particular, the Texas Attorney General has emerged as a significant regulatory enforcement authority for data privacy. Notable enforcement actions include investigating several car manufacturers for allegedly collecting large amounts of data about drivers from their vehicles and selling this information to third parties, settling (for US\$1.4 billion) with a social media company over its alleged unauthorised capture of biometric data, notifying over 100 companies of their alleged failure to register as data brokers, and settling with an AI healthcare company for allegations about the accuracy and safety of its products in hospitals.

In early 2025, the California Attorney General announced an “investigative sweep” to inspect the compliance of “the location data industry” with the CCPA provisions regarding consumers’ right to stop the sale and sharing of personal information and right to limit the use of their sensitive personal information, including geolocation data. As noted above, the CCPA’s definition of a data sale is expansive and includes any exchange of data for consideration, not just a payment. For its part, the CPPA issued an enforcement advisory on the topic of “dark patterns”, generally referring to choices presented in consumers in unclear ways, such as how to opt out of the sale of sharing of their personal information. In 2024, the CPPA also took action against seven data brokers, with the first five cases ending in settlement. Further, the California Attorney General announced a major settlement under the CCPA where it fined a car manufacturer US\$632,500, among other penalties, for its sharing of customer personal information with ad tech companies without producing contracts that contain the necessary terms to protect privacy.

Other state regulators, such as the NYDFS, were also active. In 2024, the NYDFS required a title insurer to pay US\$1 million for alleged violations of state cybersecurity regulations for failure to ensure “full and complete implementation” of its cybersecurity policies and procedures in advance of a data breach that resulted in the exposure of customers’ non-public information.

Class action litigation under the BIPA persisted in 2024; courts recognised some limitations. For plaintiffs, court decisions allowed for actions against cloud service providers, even for plaintiffs located outside of Illinois if their data was allegedly processed within Illinois. For defendants, the U.S. Court of Appeals ruled that biometric data is subject to BIPA only when

it can identify the plaintiff, with the result that non-users of a product or service, who are anonymous to a defendant (e.g., a face in the background of a photo), may not be able to bring BIPA claims. Texas and New York also brought enforcement actions under those states' biometric privacy laws.

Finally, 2024 continued to see a surge of privacy litigation at the state level brought under state wiretap laws that impose liability on website operators and service providers. These lawsuits, asserted in different states but primarily in California, claim, among other things, that the use of conventional website and web-analytic tools such as website session replays, chatbots and pixels violate wiretapping and eavesdropping state law provisions. Over 100 lawsuits were filed in 2024 alone and this trend is likely to continue in 2025.

20.2 In your opinion, what "hot topics" are currently a focus for the data protection regulator?

We anticipate that the following topics will remain hot over the next year: state-level consumer data privacy laws and regulations as more states move laws through their legislatures with an emphasis on consumer right controls in the absence of a federal law; consideration of comprehensive data privacy and AI legislation by federal legislatures; use of dark patterns on consumers; business consideration and implementation of data minimisation techniques; issues relating to the collection, use and sharing of children's data; issues surrounding the consent to collect and use biometric information; issues surrounding the privacy and security of healthcare data; consumers' access to financial relief and other remedies

when their data protection rights are violated, even in the absence of a showing of harm; issues surrounding AdTech and "surveillance" advertising; issues relating to automated decision making fuelled by AI and machine learning; a continued focus by legislators and regulators alike on cybersecurity issues, particularly in the wake of data breaches and ransomware attacks involving significant technology vendor software and industrial operations.

In addition, transfers of bulk data have come to the forefront, particularly with regard to transfer to jurisdictions perceived as impacting consumer safety, privacy and national security. Specifically, on February 28, 2024, President Biden signed Executive Order 14117 on "Preventing Access to Americans' Bulk Sensitive Data and United States Government-Related Data by Countries of Concern" (the EO). The EO calls for the DOJ to promulgate regulations to prevent the large-scale transfer of sensitive personal data and U.S. Government-related data to "countries of concern". The "Data Security Program", which implements the EO, became effective on April 8, 2025. Among other things, the Data Security Program requires businesses and individuals to utilise general licences or apply for specific licences before sending bulk data to countries of concern, defined to include China, that would otherwise be barred under regulations proposed by the DOJ.

Note

This publication is provided for your convenience and does not constitute legal advice. This publication is protected by copyright.



F. Paul Pittman is a Partner in White & Case's international Data, Privacy & Cybersecurity legal practice. Paul advises global clients on the complex data privacy and cybersecurity use and compliance issues that often arise in the processing of consumer and business data, and in the management of information and operational technology systems. Paul also assists clients in addressing data privacy and cybersecurity considerations in developing technology, products and services, including relating to social media platforms, e-commerce, connected devices (IoT), artificial intelligence and FinTech.

Paul's practice also includes advising companies on cybersecurity risks and compliance, and guiding companies in responding to data breaches. In addition, Paul advises global clients on all data privacy and cybersecurity matters that arise in corporate transactions. Paul received a Bachelor of Science degree from Allegheny College, and a *Juris Doctor* degree from Washington and Lee University School of Law.

White & Case LLP

701 Thirteenth Street, NW
Washington, D.C. 20005-3807
USA

Tel: +1 202 729 2395
Email: paul.pittman@whitecase.com
LinkedIn: www.linkedin.com/in/f-paul-pittman



Abdul Hafiz is a Data, Privacy & Cybersecurity Associate in White & Case's New York office. Abdul provides strategic legal and business advice for a variety of commercial and financial clients. Specifically, he advises on compliance with data privacy and cybersecurity laws, including the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA), the Health Insurance Portability and Accountability Act (HIPAA), the Virginia Consumer Data Protection Act (VCDPA), the Telephone Consumer Protection Act (TCPA), the Children's Online Privacy Protection Act (COPPA), and the Illinois Biometric Information Privacy Act (BIPA). Abdul also advises global clients on data privacy and cybersecurity matters that arise in corporate transactions, including mergers, acquisitions, financings and securities offerings. Abdul holds a Bachelor of Arts from Northeastern University and a *Juris Doctor* from Fordham University School of Law. Abdul is CIPP/US qualified.

White & Case LLP

1221 Avenue of the Americas
New York, NY 10020-1095
USA

Tel: +1 212 819 2527
Email: abdul.hafiz@whitecase.com
LinkedIn: www.linkedin.com/in/abdul-hafiz-cipp-us-0b87a637



Andrew Hamm is an Associate in White & Case's international Data, Privacy & Cybersecurity legal practice. Andrew advises White & Case's global clients on the complex data privacy and cybersecurity issues that often arise in the processing of consumer and business data in the consumer, technology and financial space. Andrew's practice includes counselling companies in developing privacy and cybersecurity compliance programmes in an evolving international legal landscape. Additionally, Andrew assists clients in addressing privacy and cybersecurity issues in business operations and products. Finally, Andrew advises global clients on data privacy and cybersecurity matters in corporate transactions such as mergers and acquisitions. Andrew holds a Bachelor of Arts degree from Harvard University, a Master of Arts from Johns Hopkins University, and a *Juris Doctor* degree from the American University Washington College of Law.

White & Case LLP

701 Thirteenth Street, NW
Washington, D.C. 20005-3807
USA

Tel: +1 212 729 3007
Email: andrew.hamm@whitecase.com
LinkedIn: www.linkedin.com/in/andrew-hamm-8598495a

With one of the largest and most experienced data privacy and cybersecurity groups in the world, White & Case's global team is on hand to guide clients through the relevant data protection legislation in the jurisdictions in which they are active. Seamlessly working with their counterparts in other practice areas, our global team has the depth of resources to provide integrated, creative and practical advice on the privacy-related concerns faced by our clients, wherever they are located. Our experience spans the full range of industry sectors including financial institutions and banking, biotechnology, pharmaceuticals and chemicals, construction and engineering, consumer goods and retail, automotive, hotels and leisure, IT, telecommunications, internet and social media, manufacturing and electronics, publishing and media.

www.whitecase.com



The **International Comparative Legal Guides**

(ICLG) series brings key cross-border insights to legal practitioners worldwide, covering 58 practice areas.

Data Protection 2025 features four expert analysis chapters and 27 Q&A jurisdiction chapters covering key issues, including:

- Relevant Legislation and Competent Authorities
- Territorial and Material Scope
- Key Principles
- Individual Rights
- Children's Personal Data
- Registration Formalities and Prior Approval
- Appointment of a Data Protection Officer
- Appointment of Processors
- Marketing
- Cookies
- Restrictions on International Data Transfers
- Whistle-blower Hotlines
- CCTV
- Employee Monitoring
- Data Security and Data Breach
- Enforcement and Sanctions
- E-discovery/Disclosure to Foreign Law Enforcement Agencies
- Artificial Intelligence