Client Alert | Data, Privacy & Cyber Security / Technology

Introduction of new EU General Data Protection Regulation: final stages

December 2015

Authors: Detlev Gabel, Rob Blamires, Tim Hickman

The EU institutions have completed 'trilogue' negotiations on the text of the General Data Protection Regulation, bringing the new European data protection regime very close to final

On 17 December 2015, an extraordinary meeting of the European Parliament Committee on Civil Liberties, Justice and Home Affairs voted (as expected) in favour of the likely final text of the General Data Protection Regulation ("**GDPR**"), which had been agreed two days previously at the culmination of the EU legislative institutions' trilogue negotiations. As Jan Philipp Albrecht, the Parliament Rapporteur for the GDPR, has announced on social media, all of the major outstanding issues have been agreed (although, as the European Parliament's press release clarified, before the GDPR becomes law a few formalities remain, which are not expected to be completed before February 2016).

Key changes and business impact

The GDPR brings significant changes to EU data protection law, many of which greatly impact businesses:

- **Significant new fines:** Maximum fines of the greater of **€20 million** or **4% of annual global turnover** *per* breach (a dramatic increase from the current typical maximum of less than €1 million).
- **Broader territorial reach:** Even businesses outside the EU will be subject to the GDPR, if they are offering goods or services to, or monitoring the behaviour of, EU residents (currently they are only caught if they operate data processing equipment in the EU). See further on this below.
- **Data breach reporting:** In most cases breaches will have to be reported within **72 hours**.
- **Stronger rights for individuals:** Individuals will have stronger rights against businesses, including the 'right to be forgotten'. Re-using existing data for new purposes will also become more difficult.
- **Consent harder to obtain:** Consent will always have to be express/opt-in (a 'clear affirmative action') whereas, under the existing regime, implied/opt-out consent is sometimes sufficient.
- **Data Protection Officers:** Most businesses that regularly monitor individuals, or regularly process sensitive personal data, will have to formally appoint an independent Data Protection Officer.
- **Personal data of children:** Businesses will have to obtain parental consent to process personal data of children under 16 years old (although there is scope for Member States to bring this age down as low as 13). Parental consent will be difficult/impractical to evidence, especially in an online context.
- **Impact assessments:** Whenever a business is contemplating a new activity that poses material privacy risks, it will have to conduct an impact assessment, and, if the results of the assessment indicate a high risk, obtain a prior review by the relevant Data Protection Authority.
- **Processor liability:** For the first time, data processors (i.e. businesses processing personal data solely for and on the instructions of data controllers) will have direct regulatory obligations/liability. Some of the changes will also potentially ease the burden for businesses:

- **The 'one-stop-shop':** A business that processes personal data of residents of multiple EU Member States will have a 'lead' Data Protection Authority (generally the Authority for the Member State in which it has its EU Headquarters) and, in most cases, will deal only with that Authority regarding all compliance obligations (in any Member State).
- **Greater consistency:** In theory, businesses will face a more harmonised set of compliance requirements, and a more consistent set of enforcement procedures, across the EU. In practice, this depends on the new 'consistency mechanism', which requires Data Protection Authorities to make consistent enforcement decisions (and, in any event, several areas remain unharmonised, including processing for employment law and national security, and exemptions for free speech / journalism).
- **No system of registration:** Under the current system, controllers are required to register with Data Protection Authorities. Under the GDPR, controllers will instead be required to maintain internal records of their processing activities (for disclosure on demand to Data Protection Authorities).

Why are these changes being made?

The EU's existing data protection regime is set out in Directive 95/46/EC (the "**Directive**"). The Directive (as with all EU Directives) had to be implemented into each Member State's national laws, inevitably resulting in inconsistencies and a 'patchwork' of similar but not identical requirements across the EU. Also, rapid technological developments and globalisation have rendered the Directive outdated and inappropriate for the exponential increase in the scale and types of data collection activities and cross-border data flows.

By removing the need for national implementation, and requiring Data Protection Authorities to work together more closely and consistently, the GDPR is intended to create greater harmonisation across the EU and provide more consistent protection for personal data processed within the EU and exported to third countries.

Which businesses are affected?

The GDPR applies to all businesses (regardless of economic sector or business activity) that are: (a) established in the EU, or otherwise subject to EU law; or (b) established outside the EU, but either: (i) offering goods or services to EU residents; or (ii) monitoring the behaviour of EU residents (capturing many non-EU businesses that might not be subject to the current regime).

When will the GDPR come into force?

Once formally approved by the European Parliament, the GDPR will come into force two years after publication in the EU's Official Journal. Publication is likely to be in the first quarter of 2016, so the GDPR is likely to come into force in the **first quarter of 2018**.

What should businesses do to prepare for the GDPR?

Existing Member State national data protection laws will continue to apply until the GDPR comes into force. However, during this intervening period, Data Protection Authorities are likely to begin approaching compliance issues in accordance with the GDPR. Businesses are therefore advised to start making serious strides toward compliance with the GDPR as swiftly as possible. Businesses that fail to plan and budget for the necessary changes early enough may find they are left with insufficient time and resources to achieve compliance with the GDPR – and avoid its significant penalties. Further analysis on the impact of GDPR will follow on the White & Case Technology Newsflash.

Detlev Gabel
Partner, Frankfurt
T +49 69 29994 1528
M +49 17 94555 570
E dgabel@whitecase.com

Robert Blamires
Counsel, Silicon Valley
T +1 650 213 0348
M +1 650 815 1061
E robert.blamires@whitecase.com

Tim Hickman
Associate, London
T +44 207 532 2517
M +44 7900395575
E tim.hickman@whitecase.com