PANORAMIC

ONLINE SAFETY REGULATION

European Union

LEXOLOGY

Online Safety Regulation

Contributing Editors

Jenna Rennie, Rory Hishon and Alexander Beaton

White & Case LLP

Generated on: March 31, 2026

Contents

Online Safety Regulation

Contributors

European Union

White & Case LLP

WHITE & CASE

Rory Hishon	rhishon@whitecase.com
Jenna Rennie	jenna.rennie@whitecase.com
Joseph Carroll	joseph.carroll@whitecase.com
Ben Harris	ben.harris@whitecase.com

LEGAL FRAMEWORK

Legal regime

Does your jurisdiction have a legal regime governing or addressing online safety? If so, how does it operate?

The European Union (the EU) has enacted a comprehensive legal regime for online safety in the form of Regulation (EU) 2022/2065, the Digital Services Act (DSA), which became generally applicable in February 2024 (or in 2023 for certain designated providers).

The DSA is directly effective across all EU member states and establishes a harmonised set of rules for providers of online intermediary services, including mere conduit services, caching services, hosting services, online platforms, very large online platforms (VLOPs) and very large online search engines (VLOSEs). It aims to create a 'safe, predictable and trusted online environment' by imposing a range of obligations on providers, depending on the nature and number of users of their services in the EU. For VLOPs and VLOSEs, these obligations include assessing and mitigating risks arising from illegal content and other systemic risks to users, including risks to children and to users' fundamental rights.

Oversight and enforcement of the DSA are carried out by national digital services coordinators (DSCs) appointed by each member state, while the European Commission (the Commission) acts as the primary regulator for VLOPs and VLOSEs. The DSA is supplemented by Commission guidelines, delegated acts, and codes of conduct. The regime is designed to be risk-based and proportionate, scaling obligations according to the size, reach and risk profile of each service. Providers of certain services are required to publish annual transparency reports and undergo independent compliance audits.

The DSA is not the only source of EU law that may impact the online safety landscape. Other legal instruments contribute to a safer online environment by targeting particular risks and strengthening protective measures across digital services. For example, the General Data Protection Regulation (the GDPR) is primarily designed to safeguard personal data and privacy, and the Terrorist Content Online Regulation (the TCO) deals with the dissemination of terrorist content online. However, given the number and variety of such laws, and the fact that they narrowly relate to particular issues or aspects of online safety, we have focused below on the DSA, as the EU's principal legislation designed to address online safety more broadly.

Law stated - 18 December 2025

Online harms covered

Which online harms are covered under the relevant legislation and how are these harms defined?

The DSA addresses a range of online harms, with particular focus on illegal content and 'systemic risks' that may arise from the use of online platforms. Illegal content is defined as any information that is unlawful under EU or member states' national law (such as terrorism, child-sexual-abuse material, hate speech and intellectual property infringement). Systemic risks include the dissemination of illegal content but extend more broadly to include risks to fundamental rights, risks to civic discourse, electoral processes and public

security, and risks to public health, minors and physical or mental wellbeing. In addition, there is an express provision addressing protection of minors and the Commission has recently published guidelines giving examples of potential harms to minors, such as content promoting self-harm, suicide, eating disorders or extreme violence.

However, the DSA does not provide an exhaustive list of illegal content or systemic risks. VLOPs and VLOSEs must conduct risk assessments (at least once a year) to identify for themselves any systemic risks stemming from the use, design or functioning of their service and its related systems.

Law stated - 18 December 2025

Online services covered

Which online services are covered under the law and how are these services defined?

The scope of the DSA is intentionally broad, covering a wide array of online services that are accessible to users in the EU. These include intermediary services (ie, mere conduit, caching and hosting services), and online platforms that store and disseminate information to the public at the request of users (eg, social media networks, online marketplaces and app stores). Online platforms and search engines that have more than 45 million monthly active users in the EU may be designated by the Commission as VLOPs or VLOSEs, in which case, they are subject to additional obligations under the DSA.

Importantly, the DSA applies to any provider whose services are offered to EU users, regardless of where the provider itself is established. Providers established outside the EU must appoint a legal representative within the EU to engage with the Commission and DSCs.

Law stated - 18 December 2025

Territorial scope

What is the territorial scope of the relevant law?

The DSA has broad territorial reach. It applies to any provider offering online intermediary services to users in the EU, regardless of the provider's location or place of establishment, and will, therefore, have extraterritorial effect for non-EU providers.

Law stated - 18 December 2025

Codes of practice

Are there any codes of practice or other non-binding guidelines or recommendations relating to online safety in your jurisdiction?

The DSA is supplemented by a range of non-binding codes of conduct and Commission guidelines. These typically provide detailed recommendations on best practices for DSA obligations, and play a significant role in shaping compliance practices and regulatory expectations. For example, in recently published guidelines concerning obligations related

to minors' safety, the Commission stated that it would use the guidelines to 'impose a limit on the exercise of its discretion whenever applying' the relevant provisions of the DSA.

While adherence to DSA codes of conduct is voluntary, compliance can serve as a mitigating factor in enforcement proceedings and is considered evidence of good-faith efforts to meet DSA obligations. The codes and guidelines may be updated to reflect emerging risks and technological developments, ensuring that the regulatory framework remains responsive and effective.

Law stated - 18 December 2025

Harmful versus illegal content

How does the law in your jurisdiction distinguish between harmful and illegal content?

The DSA draws a clear distinction between illegal content (meaning any content that is prohibited under EU or national member state law) and other content that service providers are expected to address. As an example, article 16 requires providers to establish a 'notice and action' mechanism for users to report content that the report considers to be illegal. This requirement only applies to illegal content – it does not extend to other types of harmful but legal content (eg, content that is offensive or that violates the service's terms and conditions).

However, while the DSA does not define 'harmful' content per se, it includes a number of requirements that are relevant to providers' handling of such content. For example, article 28 DSA requires providers to implement 'appropriate and proportionate' measures to ensure a high level of safety, security and privacy for children, which would likely include measures to protect children from harmful content. Additionally, providers of VLOPs and VLOSEs must assess and mitigate systemic risks – such as threats to electoral processes or harm to vulnerable users – which will include risks that arise from legal but 'harmful' content.

Law stated - 18 December 2025

Extremist and terrorism-related content

How does your jurisdiction regulate the dissemination of extremist and terrorism-related content online?

The DSA's duties relating to illegal content - including the notice and action mechanisms - apply to any terrorism-related content that amounts to an offence under EU or national member state law.

The DSA also requires VLOPs and VLOSEs to assess and mitigate systemic risks associated with the dissemination of terrorist content. This includes evaluating how their services might be used to spread extremist material and implementing measures to prevent such risks.

Additional requirements are imposed for certain providers under terrorism-specific legislation, particularly Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online (the TCO). The TCO defines terrorist content as material that incites, solicits or contributes to terrorist offences. The duties imposed by the TCO include

requirements to take proactive measures to prevent terrorist content appearing on a service, and to remove such content within one hour of receiving a removal order from a competent authority.

Law stated - 18 December 2025

Disinformation versus misinformation

How, if at all, does the law in your jurisdiction distinguish between misinformation and disinformation online? Does it include malinformation?

The DSA recognises the challenges posed by both disinformation and misinformation online and requires VLOPs and VLOSEs to assess and address these issues as part of their systemic risk assessment and mitigation obligations. While not expressly defined under the DSA, 'disinformation' is understood as false or misleading content that is disseminated with the intent to deceive or cause harm, while 'misinformation' refers to false or misleading content shared without malicious intent.

The Commission has issued guidelines for VLOPs and VLOSEs on the mitigation of systemic risks for electoral processes under article 35 of the DSA, which emphasise tackling disinformation and misinformation during electoral processes. The guidelines recommend that platforms implement robust mitigation measures, such as providing users with access to official electoral information, collaborating with independent fact-checkers, and clearly labelling or demoting content identified as false or misleading. They also encourage platforms to support media literacy initiatives to help users recognise and resist disinformation, and to adapt recommender systems to reduce the amplification of deceptive content. These measures are to be balanced with the protection of fundamental rights.

In addition, the Code of Conduct on Disinformation (COCD) sets out voluntary commitments for service providers to tackle the spread of false and misleading information online. For example, signatories commit to preventing the misuse of advertising systems to spread disinformation, strengthening efforts around media literacy and empowering users with tools to help them assess the provenance of digital content. Although adherence to the COCD remains voluntary, platforms that sign up are expected to implement its measures in good faith and report regularly on their progress. The DSA encourages participation in such codes as part of a broader strategy to foster accountability and transparency in the digital ecosystem.

Law stated - 18 December 2025

OBLIGATIONS FOR ONLINE SERVICE PROVIDERS

General obligations

What general legal obligations relating to safety are imposed on providers of online services, including providers of online intermediary services?

The Digital Services Act (DSA) establishes a tiered framework of obligations that reflects the different risk levels associated with different types of services.

Mere conduit and caching service providers are subject to the least burdensome requirements. Providers of hosting services, which store user-generated content (eg, web hosting services and cloud storage services), face more extensive obligations. They must implement notice and action mechanisms, allowing users and authorities to report illegal content. They are also required to publish annual transparency reports detailing their content moderation practices and enforcement actions, and to maintain clear terms and conditions that inform users about their rights and responsibilities.

Very large online platforms (VLOPs) and very large online search engines (VLOSEs) are subject to the most stringent requirements. VLOPs and VLOSEs must conduct regular, comprehensive risk assessments to identify and evaluate systemic risks stemming from their service, including the spread of illegal content and harms to minors and other vulnerable users. They are required to implement reasonable, proportionate and effective mitigation measures, such as adapting the design, features or functioning of their service, or adapting content moderation processes. They are also required to provide more extensive transparency reports, undergo independent audits, give regulators access to relevant data for supervisory purposes, and cooperate with trusted flaggers and civil society organisations.

Law stated - 18 December 2025

Risk assessments and mitigation

Are there any specific legal obligations for online service providers to conduct risk assessments and mitigate risks to safety?

Article 34 DSA requires providers of VLOPs and VLOSEs to conduct regular 'diligent' risk assessments of risks related to illegal content and other systemic threats. Providers must carry out these risk assessments at least annually, and prior to deploying new functionalities that are likely to have a critical impact on relevant systemic risks.

Article 35 requires providers to put in place reasonable, proportionate, and effective risk mitigation measures, based on and 'tailored to' the findings of their risk assessments. These measures could include adapting content moderation systems, improving user reporting mechanisms and enhancing transparency tools. Providers must also publish reports detailing their risk assessments and mitigation measures.

Additionally, providers of online platforms accessible to minors must put in place appropriate and proportionate measures to ensure a high level of privacy, safety and security of children on their service, per article 28. The Commission has recently published guidelines recommending particular measures, such as age-appropriate content controls, privacy settings and safeguards against profiling. Providers should conduct a dedicated risk review to identify potential harms to children, including risks to privacy, exposure to harmful content and other safety concerns, and determine appropriate mitigation measures. Providers are also expected to ensure that their services do not facilitate harmful interactions or expose minors to inappropriate content, and to regularly review and update their protective measures in line with evolving risks and best practices.

Law stated - 18 December 2025

Protection of minors and age verification

Are there any specific legal obligations to protect minors online? If so, what measures are required or advised, such as age verification?

The DSA includes a number of requirements relating to the protection of minors online. Providers whose services are likely to be accessed by minors are required to implement age-appropriate safety measures, including effective age assurance mechanisms such as age verification or estimation, parental controls, and content filters to prevent access to harmful material. Risk assessments should specifically address the risks to different age groups and consider how service design and features may impact children's exposure to harmful content.

The Commission's article 28 guidelines distinguish between age estimation and age verification on the basis of their accuracy, with age verification (eg, via official documents or biometric checks) offering a higher degree of certainty about a user's age than age estimation (eg, via analysing behavioural or technical signals). The guidelines encourage providers to use age estimation where it is sufficient and less intrusive but recognise that age verification may be necessary for higher-risk scenarios where greater certainty is required. Providers are advised to choose the most appropriate method based on the risk profile of their service, balancing the method's effectiveness against children's rights (eg, the right to privacy).

Law stated - 18 December 2025

Civil and human rights

Are there any obligations for online service providers to balance civil and human rights, such as privacy rights and freedom of expression, with safety regulations? If so, what measures are required or advised?

The DSA obliges all online service providers – including VLOPs and VLOSEs – to balance their compliance measures with the protection of fundamental rights, including privacy, freedom of expression and non-discrimination. The DSA also requires providers to act in a non-arbitrary and non-discriminatory manner, respecting the Charter of Fundamental Rights and considering the legitimate interests of all parties affected.

Recommended measures to protect fundamental rights include making terms and conditions clear and accessible (especially for minors), processing notices of illegal content in a timely and transparent way, and ensuring that interventions are limited to specific content rather than broadly restricting lawful material.

Law stated - 18 December 2025

Disinformation and misinformation

Are there any specific legal obligations to combat disinformation and misinformation online? If so, what measures are required or advised?

The DSA requires VLOPs and VLOSEs to assess and mitigate systemic risks arising from the spread of false or misleading information, especially where such content could impact democratic processes, public health, or the protection of minors.

Under article 34, VLOPs and VLOSEs must conduct regular risk assessments to identify how their services may facilitate the dissemination of disinformation or misinformation. Article 35 then obliges them to implement reasonable, proportionate and effective risk mitigation measures. These may include cooperating with trusted flaggers and fact-checkers, adapting recommender systems to reduce the amplification of false content, providing users with tools to report or challenge disinformation, and supporting media literacy initiatives. Services are also encouraged to participate in the Code of Conduct on Disinformation, which sets out voluntary commitments to combat disinformation (eg, by preventing the misuse of advertising systems for disinformation, strengthening media literacy and empowering users to assess the provenance of digital content).

Law stated - 18 December 2025

Notice and takedown

Is there a legislative 'notice and takedown' mechanism or similar in your jurisdiction? If so, how does it operate?

Article 16 DSA requires hosting service providers to put in place mechanisms that allow any individual or entity to notify them of specific items of content that they consider to be illegal. Mechanisms must be easy to access and use, and enable the provision of sufficiently precise and adequately substantiated reports. Upon receipt of a sufficiently substantiated report, a provider may be considered on notice of illegal content, such that it can no longer rely on the hosting defence set out in article 6 DSA.

The provider must tell the reporter of its decision regarding the article 16 notice. Under article 17 DSA, it must also tell the user who uploaded the content if it has restricted the visibility of the content (including removing or disabling content), or otherwise suspended or terminated monetisation of that content, the user's access to the service, or access to the user's account.

Providers must process notices in a timely, diligent and non-arbitrary manner, and ensure that their actions are targeted at the specific content identified in the notice. Providers must also publish annual transparency reports with information about such notices, including the number of notices received and the actions taken in response.

Separately, under article 9 DSA, member state authorities can send providers orders to remove specific items of illegal content. The order must be based on applicable national or Union law. On receipt of such an order, the provider must notify the member state authority of the effect given to the order (if any).

Law stated - 18 December 2025

ENFORCEMENT AND PENALTIES

Enforcement

How is the online safety regime enforced in your jurisdiction?

The Digital Services Act (DSA) is primarily enforced by national digital services coordinators (DSCs), who oversee compliance by providers established in their member state. DSCs have the powers to investigate, obtain information, issue orders and impose penalties for non-compliance. The Commission acts as the competent authority for very large online platforms (VLOPs) and very large online search engines (VLOSEs), with powers to supervise compliance, obtain information, conduct audits and investigations, and impose fines or remedial measures.

In addition to regulatory enforcement, individuals and entities affected by breaches of the DSA may seek private enforcement through the courts, in accordance with national judicial procedures.

Law stated - 18 December 2025

Authorities

Which authorities are responsible for enforcement? What is the basis, nature and extent of their enforcement powers?

The DSA is enforced by national DSCs in each member state and by the Commission.

Law stated - 18 December 2025

Penalties and liability

What are the potential fines or penalties for non-compliance? Are there risks of liability for employees or directors of online service providers?

For serious breaches of the DSA, such as failing to comply with key obligations or regulatory orders, fines may be imposed up to a maximum of 6 per cent of the provider's annual worldwide turnover. For less serious breaches, such as supplying incorrect information in response to a formal request for information, fines may be imposed up to a maximum of 1 per cent of annual worldwide turnover. Fines may also be imposed on a rolling basis, up to a maximum of 5 per cent of the average daily worldwide turnover for each day of non-compliance.

The DSA's enforcement regime targets the provider as a legal entity, rather than imposing liability on individual employees or directors.

Law stated - 18 December 2025

DISPUTES

Claims

What claims relating to online safety are available and most common in your jurisdiction?

Article 54 of the Digital Services Act (DSA) provides that private litigants have the right to bring claims for compensation in respect of any damage or loss suffered due to an infringement of the DSA. Any such claim would be brought in individual member states.

Article 21 DSA also provides for a non-binding out-of-court dispute settlement system, where people affected by an online platform provider's decision regarding whether to restrict specific items of content, or impose certain other restrictions referred to in article 20, can seek to resolve the dispute. A number of dispute settlement bodies have been certified for this purpose.

Law stated - 18 December 2025

Procedure

What is the procedure for claimants to bring actions relating to online safety in your jurisdiction?

Claimants may initiate proceedings before the competent national courts in their member state. This typically involves submitting a claim or complaint that details the alleged non-compliance by the provider, provides relevant evidence, and specifies the remedy sought.

Claimants may alternatively use the out-of-court dispute settlement mechanism provided for under the DSA. This allows users to refer disputes with providers of online platforms – such as disagreements over content moderation decisions or access restrictions – to a certified, independent and impartial dispute settlement body. The process is designed to be accessible and efficient, and providers are required to cooperate with the dispute settlement body. Each dispute settlement body publishes its own rules of procedure. The decisions of these bodies are non-binding, but claimants retain the right to pursue the matter further through the courts if they are dissatisfied with the outcome. This aims to offer claimants a quicker and less formal alternative to court proceedings.

Law stated - 18 December 2025

Remedies

What interim and substantive remedies may be imposed in relation to online safety claims?

Available remedies will depend on the member states' national courts. However, article 54 provides that users shall have a right to seek compensation in respect of any damage or loss suffered due to an infringement.

Law stated - 18 December 2025

Defences and exemptions

Does your jurisdiction provide any defences or exemptions from liability for online safety claims? If so, how do they operate and which online services providers may avail of them?

The safe harbour exemptions in the DSA, which stem from the EU E-Commerce Directive, generally protect intermediary service providers from liability for third-party content, provided that they act promptly to remove illegal material once they have actual knowledge of it, or awareness of facts or circumstances from which the illegality is apparent. The DSA also maintains the prohibition on general monitoring obligations, meaning providers are not required to proactively monitor all user activity or content on their services.

Law stated - 18 December 2025

UPDATE AND TRENDS

Key trends and future developments

What are the most noteworthy recent trends and developments in online safety regulation in your jurisdiction? What developments are expected in the coming year?

Recent regulatory activity has focused on strengthening child safety online, with the Commission consulting on an Action Plan against cyberbullying and gathering evidence on effective strategies to protect minors. This is complemented by ongoing work on age-verification solutions, guidelines under article 28 of the Digital Services Act (DSA), and research into the impact of social media on youth mental health.

Enforcement is also evolving, with the Commission conducting investigations into very large online platforms (VLOPs) and very large online search engines (VLOSEs) that may result in stricter oversight and clearer standards for systemic risk management and transparency. The Commission is expected to further clarify and potentially strengthen its enforcement powers following the conclusion of these investigations.

Rules on the procedures for DSCs to grant data access to researchers are being operationalised, with VLOPs and VLOSEs required to provide vetted researchers with access to a potentially wide range of platform data. This is intended to support independent scrutiny of VLOPs' identification and mitigation of systemic risks.

Additionally, the Commission is continuing to conduct public consultations regarding the DSA's obligations, for example, in relation to the article 18 requirements to notify law enforcement or judicial authorities in a member state about threats to life or safety. This consultation aims to clarify the scope of criminal offences, notification procedures and reporting requirements to ensure consistent application across member states.

Law stated - 18 December 2025