PANORAMIC

ONLINE SAFETY REGULATION 2026

Contributing Editors

Jenna Rennie, **Rory Hishon** and **Alexander Beaton**

White & Case LLP

LEXOLOGY

Online Safety Regulation 2026

Contributing Editors

Jenna Rennie, Rory Hishon and Alexander Beaton

White & Case LLP

A comparative guide to online safety regulation in key jurisdictions worldwide. Topics covered include the legal framework for combating online harms; obligations for online service providers, including risk assessments and mitigation; enforcement and penalties; and disputes, including remedies and defences.

Generated on: January 14, 2026

Ireland

Connor Cassidy, **Sarah Jayne Hanna**, **Simon Shinkwin**
Matheson

Summary

LEGAL FRAMEWORK

Legal regime

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

In Ireland, there are three key pieces of legislation which address different aspects of online safety, as follows:

- Online Safety and Media Regulation Act 2022 (the OSMR): on the application of traditional media regulation to online platforms and the establishment of a media and online safety regulator;
- Digital Services Act 2024 (the DSA): on the safety and predictability of the online environment and the balancing of online safety and innovation; and
- Regulation (EU) 2021/784 (the TCOR) on addressing the dissemination of terrorist content online.

Pursuant to the powers afforded it under the OSMR, Coimisiún na Meán (CnaM) has also introduced the Online Safety Code 2024 (the OSC), which imposes binding obligations on video-sharing platform service providers to provide adequate protections for children and the public from harmful and illegal content.

Law stated - 6 January 2026

Online harms covered

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

The DSA covers a broad range of online harms, including illegal content (like child abuse material, terrorism and hate speech), as well as harmful content that it not illegal, for example, risks to public health.

The TCOR covers content that may ultimately pose a threat to the security and safety of persons and the fundamental rights of persons, for example, the right to respect for private life and to an effective remedy.

The OSC, which applies strictly to video-sharing platforms, sets out specific grounds upon which audiovisual commercial communications (ACCs) may be harmful to the general public (eg, ACCs that encourage behaviour prejudicial to health or safety). The OSC also sets out audiovisual commercial communications that are specifically harmful to children and makes provision for the potential adverse effects that online content may have on the physical, mental or moral development of children.

Law stated - 6 January 2026

Online services covered

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

The DSA applies to intermediary service providers (ISPs), including very large online platforms (VLOPs) and very large online search engines (VLOSEs). Designated VLOPs based in Ireland include Apple, Google, Shein, LinkedIn, Meta (Facebook and Instagram), Pinterest, TikTok, Temu and X, and designated VLOSEs based in Ireland include Microsoft's Bing and Google Search.

The OSC covers video-sharing platform services based in Ireland, defined under section 3(3)(2) of the OSMR. The TCOR covers platforms, known as hosting service providers, that host and store data. However, it does not apply to private messages, meaning that private messages cannot be monitored by hosting service providers for the purposes of the TCOR.

Law stated - 6 January 2026

Territorial scope

4 | What is the territorial scope of the relevant law?

The OSMR and the OSC apply to service providers established in Ireland, as well as service providers that have a parent or subsidiary undertaking established in Ireland and service providers that are part of a group, of which another undertaking in the same group is established in Ireland.

The DSA applies to a wide range of intermediary services providers that offer services to users within the European Union, regardless of where the service provider is established. Even if a service provider is based outside the European Union, it must comply with the DSA if it offers services to recipients who are located or established in the European Union. In Ireland, the DSA is supplemented at national level by the Digital Services Act 2024.

The TCOR applies to hosting service providers whose main establishment is located in Ireland, as well as hosting service providers who provide services in Ireland, including service providers whose main establishment is located in a different EU member state.

Law stated - 6 January 2026

Codes of practice

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

In October 2024, CnaM published its Online Safety Guidance Materials, drafted to assist video-sharing platform service providers in their implementation of the necessary measures as set out in the OSC.

In respect of the TCOR, CnaM has published its Decision Framework setting out the process to be followed in order for a decision to be made under the TCOR and key obligations for hosting service providers that are found to be exposed to terrorist content.

Guidance published by the European Commission in respect of the DSA is also applicable in Ireland.

Law stated - 6 January 2026

Harmful versus illegal content

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

CnaM defines harmful content as: cyberbullying, pornography, gross violence, dangerous challenges, promotion of eating disorders, promotion of suicide or self-harm content – where the harm creates a risk to a person's life or health. Conversely, the OSC lists the following as illegal content: child sexual abuse material, child trafficking, terrorist content, offences concerning racism / xenophobia or incitement to violence or hatred against a group of persons on protected grounds (gender, political affiliation, disability, language, ethnic minority membership, religion, age or sexual orientation).

Law stated - 6 January 2026

Extremist and terrorism-related content

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

The dissemination of extremist and terrorism-related content online is principally regulated by the TCOR in Ireland. Terrorist content is defined under the TCOR as one of or more of following types of material, namely material that:

- incites the commission of an offence under article 3(1) of Directive (EU) 2017/541;
- solicits a person or a group of persons to commit or contribute to the commission of an offence under article 3(1) of Directive 2017/541;
- solicits a person or a group of persons to participate in the activities of a terrorist group;
- provides instruction on the making or use of explosives, firearms or other weapons, noxious or hazardous substances, or on other specific methods or techniques for the purpose of committing or contributing to the commission of one of the terrorist offences referred to in article 3(1) of Directive (EU) 2017/541; or
- constitutes a threat to commit one of the offences referred to in article 3(1) of Directive (EU) 2017/541.

Law stated - 6 January 2026

Disinformation versus misinformation

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

In April 2025, the Irish government published its 'National Counter Disinformation Strategy' (NCDS), which applies the same definition of 'disinformation' as set out in the European Democracy Action Plan (the EDAP), defining disinformation as 'false or misleading content that is spread with an intention to deceive or secure economic or political gain and which may cause public harm'. The NCDS also applies the EDAP's definition of 'misinformation' defining the term as 'false or misleading content shared without harmful intent though the effects can still be harmful, for example, when people share false information with friends and family in good faith'.

While these definitions have not been drafted into Irish legislation, the NCDS illuminates the Irish government's position, as Ireland looks to further legislate and regulate disinformation and misinformation in online spaces.

Law stated - 6 January 2026

OBLIGATIONS FOR ONLINE SERVICE PROVIDERS

General obligations

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

An overview of the key obligations placed on the providers of online services under the Digital Services Act (DSA), the Online Safety Code 2024 (OSC) and Regulation (EU) 2021/784 (the TCOR) is outlined below.

Digital Services Act

The DSA establishes a tiered system of obligations based on the nature and size of the services offered by the provider. At a high level, these include the following categories of providers:

- intermediary service providers: providers who offer a 'caching', 'hosting' or 'mere conduit' service. ISPs are required to:
    - establish a single point of contact with (1) relevant national authorities, the EU Commission and the European Board for Digital Services and (2) users of their services;
    - implement terms and conditions which identify any restrictions imposed in relation to the use of their services; and
    -

publish annual reports regarding content moderation activities engaged in over the previous 12 months, information relating to illegal content, use of automated tools and complaints received from users;

- hosting services: services that consist of the storage of information provided by and at the request of a recipient of the service. In addition to the obligations imposed on ISPs, hosting service providers are required to:
    - implement a 'notice and action' mechanism which allows for individuals and entities to notify them of the presence of allegedly illegal content;
    - provide a statement of reasons to the affected user where an action has been taken on the grounds of a report of illegal content or content incompatible with the provider's T&Cs; and
    - notify law enforcement/judicial authorities regarding any information that gives rise to a threat to the life or safety of a person;
- online platforms: hosting services that at the request of a recipient of the service, stores and disseminates information to the public (unless that activity is a minor and purely ancillary feature of another service). In addition to the obligations imposed on ISPs and hosting service providers, online platforms must:
    - implement an internal complaint-handling system to allow users lodge complaints regarding content moderation actions taken against them;
    - prioritise notices submitted by 'trusted flaggers' regarding illegal content;
    - take measures against recipients of the service who frequently provide illegal content and against users who frequently submit unfounded complaints;
    - design their online interface and organisation in a manner that does not impair a user's ability to make free and informed decisions;
    - ensure that users can clearly identify information which constitutes advertising and include information about recommender systems in the provider's T&Cs (where used); and
    - include certain additional categories of information in their annual transparency reports;
- Providers of online marketplaces must, in addition to the obligations set out above for online platforms:
    - only allow traders to use the marketplace once they have provided the necessary information; and
    - ensure the online interface design enables traders compliance with relevant EU law rules.

VLOPs and VLOSEs are online platforms and search engines that have been designated by the European Commission as exceeding 45 million average monthly users. In addition to the obligations set out above in respect of online platforms, providers of VLOPs and VLOSEs must conduct assessments of systemic risk on their platform and implement

mitigation measures in respect of such risks. VLOPs and VLOSEs are also required to establish a dedicated compliance function including a head of compliance and to conduct annual independent audits to assess their compliance with the obligations of the DSA. VLOPs and VLOSEs must also include additional information in their transparency reports regarding content moderation resources, and must report twice annually (as opposed to once per year for online platforms).

Online Safety Code

The OSC imposes additional obligations for video-sharing platform service (VSPS) providers. The OSC requires VSPS providers to take measures appropriate to the size of the platform and nature of the service to protect children and the general public from harmful content generally, and certain prescribed forms of content, including cyberbullying, promotion of sharing methods of self-harm or suicide, criminal content (such as child sexual abuse material) and adult-only content.

In particular, under the OSC, obligations in the OSC require VSPS providers to:

- implement T&Cs that contain sufficient restrictions to prohibit illegal content;
- have due regard for the fundamental rights of parties involved in the event of suspending an account;
- implement age assurance measures for adult-only video content;
- establish an easy-to-use content rating system which enables users to rate the content as not suitable for children;
- ensure that any third-party advertisements on their platforms do not contain harmful or restricted content;
- provide for parental control systems on the platform with regard to video content; and
- include a mechanism to allow users to report and flag restricted or harmful video content.

TCOR

Under the TCOR, certain designated hosting service providers are obliged to act expeditiously to remove content which advocates, solicits, threatens or incites terrorism. The designated hosting service providers are required to remove such content within one hour of receiving a removal order from Coimisiún na Meán (CnaM). CnaM is responsible for deciding whether hosting service providers are exposed to terrorist content and for imposing penalties on providers for non-compliance.

To date, CnaM has determined that five of the 10 designated hosting service providers under the TCOR are exposed to terrorist content, and therefore subject to the removal requirements.

Law stated - 6 January 2026

Risk assessments and mitigation

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

Yes, under the DSA, VLOPs and VLOSEs are specifically required to conduct risk assessments and implement risk mitigation measures. VLOPs and VLOSEs must assess and mitigate the following risks within their systems:

- the dissemination of illegal content through their services;
- any actual or foreseeable negative effects for the exercise of fundamental rights;
- any actual or foreseeable negative effects on civil discourse and electoral processes, and public security; and
- any actual or foreseeable negative effects in relation to gender-based violence, the protection of public health and minors and serious negative consequences to the person's physical and mental wellbeing.

Law stated - 6 January 2026

Protection of minors and age verification

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

Under the DSA, 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 for minors. Such platforms shall not present advertisements on their interface which are based on profiling, when they are aware the recipient of such is a minor. Further, the European Commission has recently published guidelines that assess compliance with such obligations.

VLOPs and VLOSEs must also consider any negative effects upon minors within their systemic risk assessments and mitigation measures.

Providers of intermediary services primarily directed at or used by minors must also ensure that their T&Cs and/or any restrictions are explained in a way that minors can understand.

In addition to the DSA, the OSC sets out specific obligations for VSPS providers, with a particular emphasis on the protection of minors against harmful content online. As a means of protecting minors online under the OSC, VSPS providers must implement certain measures, appropriate to the size of the platform and nature of the service. In particular, the OSC sets out certain protections directed at ensuring the safety of minors online, including requiring VSPS providers to include appropriate age assurance measures in respect of adult-only video content, requiring the establishment of an easy-to-use content rating system, and inclusion of parental control systems for video content.

Law stated - 6 January 2026

Civil and human rights

12 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?

Yes, the DSA requires that when providers of intermediary online services impose restrictions on users in respect of content moderation, such providers must have due regard to the legitimate interests of all parties involved, including the fundamental rights of the recipients of the service. Such restrictions may include prohibitions on harmful content. Further, VLOPs and VLOSEs that are required to carry out systemic risk assessments and implement mitigation measures must take into consideration any potential risks that may negatively affect fundamental rights within their systems.

Recent guidelines adopted by the European Data Protection Board, however, clarified that the DSA aims to complement the rules of the GDPR to ensure the highest level of protection of fundamental rights in the digital space.

Law stated - 6 January 2026

Disinformation and misinformation

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

The EU's 2022 Code of Conduct on Disinformation (the Disinformation Code) is a voluntary framework, agreed upon by a number of relevant stakeholders, to address the spread of disinformation online. The Disinformation Code has now been integrated into the DSA framework, meaning it is now a relevant benchmark for determining DSA compliance regarding disinformation risks for the providers of VLOPs and VLOSEs that adhere to and comply with its commitments. In particular, the Disinformation Code focuses on:

- demonetising purveyors of disinformation;
- implementing transparent political advertising through efficient labelling;
- reducing manipulative behaviour, such as through fake accounts and bots;
- empowering users to navigate safely online and make informed decisions;
- fact-checking coverage throughout the EU; and
- proving data access for researchers.

In addition, Regulation (EU) 2024/1689 (the AI Act) requires that deployers of certain AI systems that generate 'deep fakes' or AI generated/manipulated images, video or audio content that resembles existing persons, places etc and that would falsely appear to be authentic, must disclose that such content is artificially generated or manipulated.

Law stated - 6 January 2026

Notice and takedown

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

Pursuant to the DSA, providers of hosting services are required to implement a 'notice and action mechanism' on their service which allows any individual or entity to notify the provider of the presence of illegal content on their service. In particular, the hosting service provider is required to ensure the ability of users to submit sufficiently precise and adequately substantiated notices. Providers are required to process all notices and take decisions in respect of the information to which the notices relate, in a timely, diligent, non-arbitrary and objective manner.

Where action is taken against a user or their content, the provider is required to provide a statement of reasons regarding the decision taken and information regarding redress. Where the service constitutes an online platform, the provider is also required to maintain an internal complaints system that enables the recipients of their services to lodge complaints against content or account moderation actions taken against them.

In addition, under the DSA, where a provider of an intermediary service receives an order from a national judicial / administrative authority to act against specified illegal content, the provider must inform the authority who issued that order (or any other authority specified in the order) of the effect given to the order. Where a similar order is received to provide information about a recipient of the service, the provider must similarly inform the issuing authority (or any other authority specified in the order) of the effect given to it.

Law stated - 6 January 2026

ENFORCEMENT AND PENALTIES

Enforcement

15 | How is the online safety regime enforced in your jurisdiction?

The online safety regime is principally enforced by Coimisiún na Meán (CnaM), which has competency over enforcing the Digital Services Act (DSA) (although the European Commission also exercises direct supervision of very large online platforms (VLOPs) and very large online search engines (VLOSEs), Online Safety and Media Regulation Act 2022 (the OSMR), the Online Safety Code 2024 (OSC) and Regulation (EU) 2021/784 (the TCOR) in Ireland. The Irish courts also play a role in confirming administrative penalties imposed by CnaM.

Under the DSA, recipients of the services provided by intermediary service providers also have the ability to seek compensation, in accordance with Irish law and procedure, where they have suffered loss or damage due to an infringement of their rights by those providers. In Ireland, this would be by way of civil proceedings before the Irish courts.

Law stated - 6 January 2026

Authorities

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

Coimisiún na Meán

CnaM is designated in Ireland in a number of capacities: (1) as Ireland's digital services coordinator under the DSA; (2) under the OSMR as the body responsible for regulating traditional and online media in Ireland; and (3) as the competent authority to decide whether hosting service providers are 'exposed' to terrorist content under article 5 TCOR, and to impose penalties for non-compliance with TCOR. CnaM has various supervisory and enforcement powers under the DSA, OSMR and TCOR, which include, broadly, the power to:

- investigate suspected infringements (eg, where harmful content has been reported);
- request information from platforms on their compliance;
- order inspections (including on-site checks) to verify compliance;
- issue binding commitments where platforms will agree to specific actions to resolve an issue; and
- impose administrative fines for non-compliance.

The Irish High Court and Circuit Court also have concurrent jurisdiction to confirm any administrative fines imposed by CnaM.

An Garda Síochána

An Garda Síochána is the competent authority in Ireland with sole responsibility for forcing platforms to remove terrorist content by way of 'removal orders'. Any platform served with a removal order has one hour to remove the relevant content from receipt of the order. An Garda Síochána will also send the removal order to the competent authority in the country where the platform is established.

The courts

Under article 54 of the DSA, recipients of services provided by intermediary service providers can seek compensation from those providers in respect of any damage or loss suffered due to an infringement of the DSA. A mandated legal person or body may also bring a representative action on behalf of users to exercise the rights conferred on those users by the DSA (articles 86 and 90 of the DSA).

Law stated - 6 January 2026

Penalties and liability

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

The potential fines and penalties for non-compliance depend on which framework is applicable.

- under the OSMR/OSC, CnaM can impose fines of up to the greater of €20 million or 10 per cent of the annual turnover of the provider in the financial year preceding the date of the non-compliance finding;
- under the DSA, CnaM can impose fines of up to the greater of €20 million or 6 per cent of the total worldwide annual turnover of the provider in the preceding financial year (assuming the European Commission has not already issued proceedings against the provider in question for the same specific infringement); and
- under the TCOR, failing to comply with a Removal Order issued by An Garda Síochána can result in CnaM imposing fines of up to 4 per cent of the hosting platform's annual global turnover.

There is also the potential for personal (criminal) liability for employees and directors, depending on which framework is applicable. Criminal liability for individuals is primarily a matter of national law in the EU member states. The types of actions that may result in criminal liability include: failing to comply with a request for information or an order from CnaM; obstructing CnaM during the course of an investigation; knowingly providing false or misleading information to CnaM.

In Ireland, as set out in the OSMR, the maximum penalty for employees for non-compliance is a fine of up to €500,000 and/or imprisonment for up to a period of 10 years.

Law stated - 6 January 2026

DISPUTES

Claims

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

The most common complaints which are made by users to Coimisiún na Meán (CnaM) relate to the following:

- account suspension or restriction;
- bullying and harassment;
- hate speech and hateful behaviours;
- removal or disabling access to content;
- misleading/inaccurate information;
- limiting visibility of content without notification to the user;
- restrictions on monetisation;

- lack of transparency in terms or unfair terms of service;
- defamation;
- exposure to harmful content such as self-harm promotion;
- terrorism; and
- child sexual abuse material.

Under the Digital Services Act (DSA), recipients of the services provided by intermediary service providers also have the right to seek compensation from those providers, in respect of any damage or loss suffered due to an infringement by those providers of their obligations under the DSA. The DSA is also one of the relevant legal acts included in Annex I to Directive (EU) 2020/1828 (the EU Representative Actions Directive), meaning it is amenable to forming the basis of a representative action by a qualified entity in appropriate circumstances. To date, no individual or representative action proceedings have been commenced before the Irish courts under the DSA, although the regime is still in its relative infancy.

Law stated - 6 January 2026

Procedure

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

There are a number of procedures available, depending on which framework is applicable (ie, DSA or OSMR). Claimants can make a complaint, as distinct from proceedings seeking compensation, as follows:

- Under the DSA, online platforms (including those operating in Ireland) are legally obliged to have internal complaints handling mechanisms. In the first instance, claimants can report an issue/make a complaint directly to a platform using its complaints procedure.
- Further, claimants can avail of the out-of-court dispute settlement (ODS) mechanism under the DSA. The Appeals Centre Europe (ACE) is a certified ODS body for resolving content moderation disputes with platforms. While ACE decisions are non-binding, platforms are encouraged to implement them.
- If the claimant is dissatisfied with the response from the platform arising from the internal complaints channel, or does not receive any or adequate response, they can make a report/complaint to CnaM who may investigate the matter directly or refer it to another organisation, for example, the Competition and Consumer Protection Commission.
- Claimants can also make a report to law enforcement in appropriate circumstances.

Claimants can also seek compensation from providers of intermediary services in respect of any damage or loss suffered due to an infringement by those providers of their obligations under the DSA. In Ireland, such proceedings would most likely be commenced in either the

Circuit Court or the High Court, depending on the level of damages claimed. To date, no such proceedings have been commenced.

Law stated - 6 January 2026

Remedies

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

The following interim remedies are available in Ireland:

- Interim court order: this is a temporary or urgent court order (usually an injunction) granted where there is an immediate risk of significant harm to an individual. The order compels a person or entity to remove specific online content or refrain from publishing further content until a full court hearing can take place.
- Temporary content limitation/takedown notice: these are provided for under the DSA and the Online Safety and Media Regulation Act 2022 (OSMR) and require the online platform to restrict access to or remove deemed illegal or harmful content or information.
- Ordering compliance: as part of its enforcement powers CnaM can, where an in-scope platform is found to be in breach of its obligations, issue compliance notices and orders to cease infringing acts.

The substantive remedies available in Ireland include fines and periodic penalty payments; enforcement notices (compelling online platforms to address and rectify breaches of their regulatory obligations); prosecution of senior management or employees; service blocking (where access is blocked to specific online services or content or alternatively, forcing platforms to suspend users who abuse the platform); user-level redress (which includes content removal, damages, contract termination or price reduction); and binding commitments (legally enforceable promises made by online platforms to resolve compliance issues).

Law stated - 6 January 2026

Defences and exemptions

21 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?

Ireland provides conditional exemptions from liability for online service providers under the DSA and OSMR, provided they meet certain obligations and do not play an active role in transmitting illegal content. The core principle is that providers are not under a general obligation to monitor the information they transmit or store, but must act when made aware of illegal content. For example:

- mere conduit: platforms are exempt from liability if they are only transmitting third-party content without modifying it;
- caching (ie, storing): Platforms are exempt from liability if they automatically and temporarily store content to make it more efficient to transmit, provided they do not modify the content, comply with access conditions and act fast to remove blocked content; and
- hosting: Platforms are exempt from liability if they store information provided by users, as long as they act expeditiously to remove or disable access to illegal content once they have actual knowledge of it.

Law stated - 6 January 2026

UPDATE AND TRENDS

Key trends and future developments

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

Guidance from Coimisiún na Meán (CnaM)

The findings relating to the first investigations commenced by CnaM under the OSMR are likely to be published during the course of 2026. It is anticipated that these findings will provide some future guidance as to the indicative level of fines likely to be levied by CnaM for certain non-compliance.

Designation challenges

There have been a number of recent challenges by several platforms designated as either very large online platforms (VLOPs) and very large online search engines (VLOSEs) under the Digital Services Act (DSA) by the European Commission, as intermediary service providers under the DSA at a national level by CnaM, and as video-sharing platform service providers by CnaM under OSMR. It is anticipated that these designation challenges, as well as challenges to levies imposed by the European Commission and at a national level, will continue, particularly where CnaM is continuing to establish and develop its own list of in-scope platforms.

Vetted researchers

In July the European Commission adopted the delegated act on data access under the DSA, which enables vetted researchers to obtain unprecedented access to platforms' data. We expect there to be a focus by both the European Commission and CnaM on platforms' compliance with vetted researcher access. There is also scope for increased enforcement risk arising from any systemic issues identified by vetted researchers, and brought to the attention of regulators.

Protection of minors

The protection of minors online, including the personal data of minors, has been and continues to be a key area of focus for regulators in Ireland and the EU. The Irish Data Protection Commission and CnaM recently signed a cooperation agreement and issued a joint statement regarding advancing the safety of children and protection of their personal data online. Further, the Data Protection Commission (DPC), in conjunction with the French Data Protection Authority, most recently launched an advertising campaign to educate parents in respect of the protection of children online, encouraging parents to think before sharing photos and videos of their children online. This campaign has received significant national and international attention. In addition, the European Commission recently published guidelines under the DSA that seek to promote proportionate and appropriate measures for online platforms to protect children from online risks such as grooming, harmful content, problematic and addictive behaviours, as well as cyberbullying and harmful commercial practices.

AI deployment

The deployment of AI models is receiving increased interest from regulators in Ireland and the EU. The DPC continues to engage with many of the large technology companies in relation to the development and training of AI models. In addition, CnaM is starting to make enquiries into the use of such tools when they are integrated into an online platform and generating content online.

Increased enforcement activity

It is expected that there will be an increased level of enforcement activity more generally by CnaM, and investigations in particular, throughout 2025 and beyond. CnaM has already signalled its willingness to use its investigation powers to ensure compliance where it considers that informal engagement with platforms is not achieving the desired result. Article 16 of the DSA (notice and action mechanisms) in particular has been an area of focus and is expected to remain so into 2026.

Law stated - 6 January 2026

Connor Cassidy Connor.cassidy@matheson.com
Sarah Jayne Hanna sarahjayne.hanna@matheson.com
Simon Shinkwin simon.shinkwin@matheson.com

Matheson

Read more from this firm on Lexology