

Global  
**Online Safety Regulators**  
Network

# Regulatory Index

---

Comparing international approaches and perspectives to online safety regulation



**Developed by the members of the Global Online Safety Regulators Network:**

**eSafety Commissioner** (Australia), **Online Safety Commission** (Fiji), **Arcom** (France), **Coimisiún na Meán** (Ireland),  
**Korea Communications and Standards Commission** (Republic of Korea), **Council of Media Services** (Slovakia),  
**Film and Publications Board** (South Africa), **Ofcom** (United Kingdom)

# Regulatory Index

<b>1. About the Index</b>	<b>2</b>
<b>2. Key terminology</b>	<b>3</b>
<b>3. Jurisdictional snapshots</b>	<b>5</b>
3.1 <b>Australia</b> (eSafety Commissioner)	6
3.2 <b>Fiji</b> (Online Safety Commission)	7
3.3 <b>France</b> (Arcom)	8
3.4 <b>Ireland</b> (Coimisiún na Meán)	9
3.5 <b>Republic of Korea</b> (Korea Communications and Standards Commission)	10
3.6 <b>Slovakia</b> (Council of Media Services)	11
3.7 <b>South Africa</b> (Film and Publications Board)	12
3.8 <b>United Kingdom</b> (Ofcom)	13
<b>4. Regulatory analyses</b>	<b>14</b>
4.1 Online safety regulatory remits	15
4.2 Online harms	16
4.3 Regulated entities	17
4.4 Obligations for regulated entities	18
4.5 Information gathering and enforcement	19



## About the Network

The Global Online Safety Regulators Network (the Network) is a global forum dedicated to supporting collaboration between online safety regulators, sending a strong message about our shared commitment to online safety regulation.

The Network is composed of members and observers. Members are independent statutory authorities responsible for online safety within their respective jurisdictions.

Members have a commitment to human rights, democracy, the rule of law, and are independent from political and commercial interference.

Observers are organisations with an online safety focus and remit, such as NGOs, multi-stakeholder groups, and government departments.

For more information, visit [esafety.gov.au/about-us/who-we-are/international-engagement/the-global-online-safety-regulators-network](https://esafety.gov.au/about-us/who-we-are/international-engagement/the-global-online-safety-regulators-network).

## About the Index

The Online Safety Regulatory Index (the Index) supports the Network's mission to pursue cohesive online safety regulation.

Developed by Network members, the Index is a foundational document designed to support collaboration and interjurisdictional comparison of online safety regulatory frameworks. The Index seeks to highlight areas of commonality and divergence and serves as an important resource to support broader understanding of approaches to online safety regulation.

### The Index comprises two sections:

Section one provides **jurisdictional snapshots** of each member country and their regulatory approach to online safety, highlighting relevant legislation and regulation, scope and remit, and authority and functions. The jurisdictional snapshots were drafted by each regulator separately. As such, there is some divergence in language between snapshots.

Section two provides **comparative analysis**, collating and comparing regulators' approaches to online safety regulation across key themes, such as remit, regulated online harms, regulated platforms and services, obligations for regulated entities, and enforcement.

The Index reflects a global perspective, and some concepts have been grouped together that may be described differently in different contexts, noting that local definitions, thresholds, and terminology vary between jurisdictions. Therefore, while the Index is intended to be a helpful guide, it is not a substitute for consulting domestic legislation and regulatory documents published by Network members. The Index will be updated periodically.



# Key terminology

*Please note that these key terms may have varied meaning and application in each jurisdiction.*

**Age-assurance (AA):** an umbrella term used to describe a range of techniques and technologies for proving someone's age in online environments, such as age-verification and age-estimation.

**Age-estimation (AE):** an approximate determination of someone's age using estimation technology such as photo analysis powered by artificial intelligence.

**Age verification (AV):** a determination of one's age to a high level of certainty, typically by verifying data against an external source like an identity document.

**Blocking notice:** a legal notice issued to a platform or service directing that platform or service to block domestic access to a particular piece of content that is often hosted overseas.

**Business disruption order:** an enforcement order available under the UK's *Online Safety Act 2023* that allows the appropriate court to do any number of things to 'disrupt' the business of an online platform or service. This can include withdrawal of advertisers or directing an ISP to block domestic access to the platform or service.

**Child sexual exploitation and abuse (or 'CSEA')** is a broad term that encompasses all forms of child sexual exploitation and abuse, including CSAM, CSEM, and other activities like sexual extortion and sex trafficking.

**Disinformation:** information that is knowingly or recklessly false and is designed to deliberately mislead and influence a person or group of persons for malicious or deceptive purposes.

**End-to-end-encryption (EE2E):** a method of secure communication that allows only the people communicating with each other to read the messages, images, or files being exchanged.

**Harmful algorithmic pattern:** a pattern of recommended content delivered to an end-user by a recommender system that could, in aggregate, result in significant harm (e.g. radicalisation, eating disorder, self-harm, etc).

**Harmful to youth:** content that may be damaging to the physical or psychological health or development of children or young people, such as pornography or high-impact violence (also referred to as age-inappropriate content and 'restricted content') (Republic of Korea terminology).

**Misinformation:** incorrect or false information that is spread due to ignorance, error, or mistake without the intention to deceive.

**NCII or IBA:** non-consensual sharing of intimate images (NCII) or image-based abuse (IBA) refers to the act of sharing or threatening to share intimate images of a person without their consent.

**Proactive detection:** in content moderation, proactive detection refers to the practice of scanning user-generated content proactively to detect harmful or policy violating content before it is reported by a user or authority.

**Pro-terror content:** content that advocates for the doing of a terrorist attack because it depicts, incites, promotes, glorifies, praises or otherwise sympathises with terrorist or extremist groups or activities.

**Restricted content:** content that may be damaging to the physical or psychological health or development of children or young people, such as pornography or high-impact violence (also referred to as age-inappropriate content and content harmful to youth) (Australian terminology).

**Safety by Design:** a concept that proactively places user safety and rights at the centre of product design and delivery, requiring platforms and services to forecast and mitigate online risks.

**Social media service:** an online service or platform that's primary purpose is to enable online social interaction between end-users. This may include services that allow users to interact with one another, post or generate material, or view material posted or generated by other users.



**Child sexual exploitation material** (or ‘CSEM’) is any content that presents a child in a sexual context. It includes content that sexualises and takes unfair advantage of a child, as well as content that shows sexual activity by a child.

**Child sexual abuse material** (or ‘CSAM’) shows a sexual assault against a child and can be considered a sub-set of child sexual exploitation material.

**Content removal notice / take-down notice:** a notice issued to a platform or service that directs that platform or service to remove a particular piece of content from their service or platform.

**Digital literacy:** the ability to understand technology and digital environments, identify and respond to risks, and access and use digital services and platforms safely.

**Online hate speech** or **online hate:** generally, refers to user-generated content that discriminates against an individual or group based on a protected attribute, such as race, sexuality, gender, culture, health status, or other. ‘Online hate’ is generally considered a broader term that encompasses all hateful online content and actions, including speech, imagery, video, symbolism, and other user-to-user interactions.

**Media literacy:** the ability to access, analyse, evaluate and create media and communications across a variety of contexts.

**TVEC:** terrorism and violent extremism content. Generally, TVEC refers to content that depicts or advocates for acts of violent extremism, or otherwise depicts, advocates for, promotes, incites, or sympathises for terrorist or extremist organisations, groups, or ideologies.

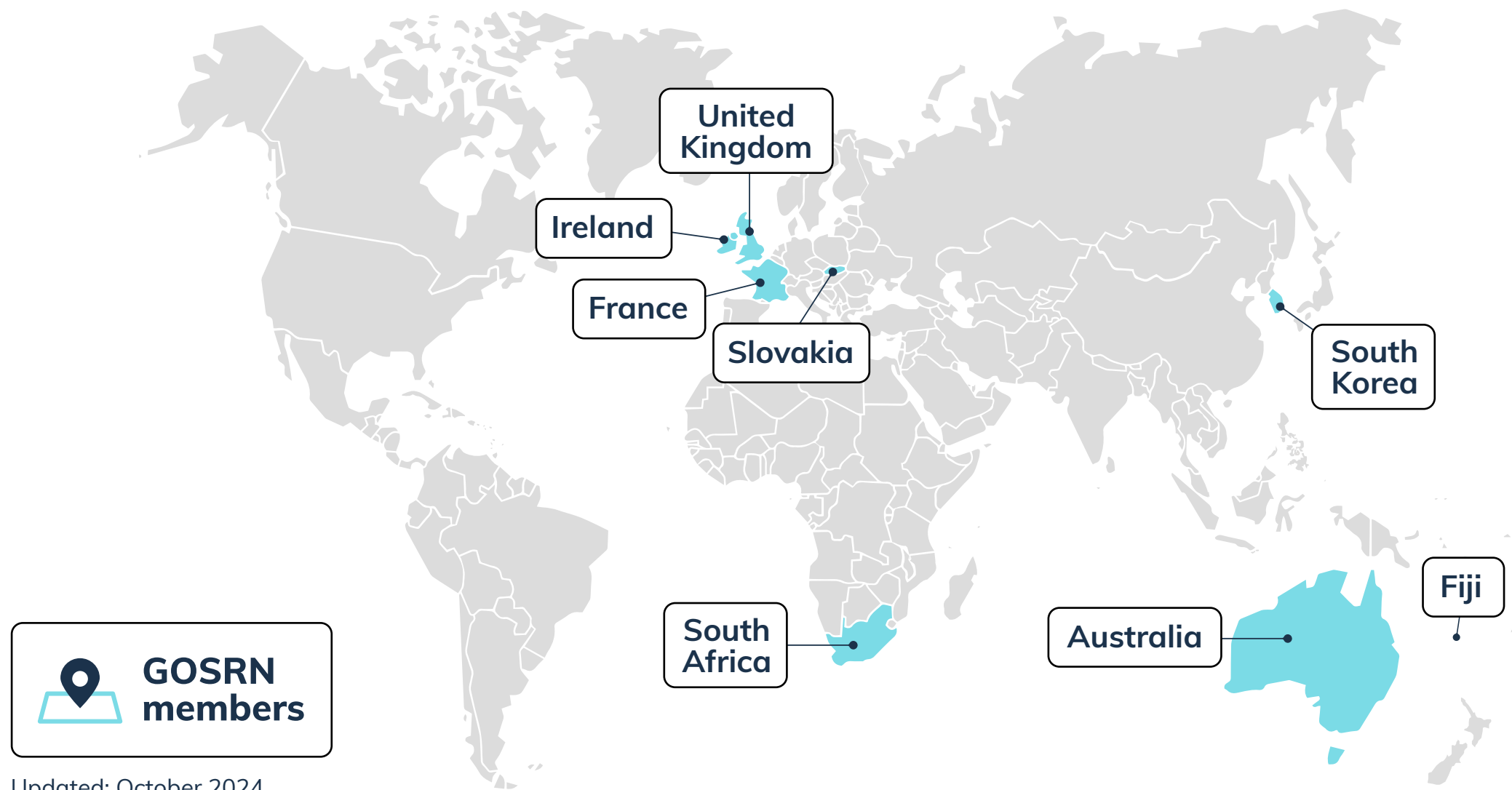
**TFGBV:** technology-facilitated gender-based violence, defined as any act that is committed, assisted, aggravated, or amplified by the use of information communication technologies or other digital tools against a person on the basis of their gender, which results in, or is likely to result in, harm or other infringements of rights and freedoms.

**User-to-user (U2U) service:** a platform or service that enables users to generate and / or share content with other users.

**Video-sharing platform (VSP):** a platform or service that allows users to generate, post, share, or interact with video content that is generated by other users (UK and EU terminology).



# Jurisdictional snapshots



# Australia: eSafety Commissioner (eSafety)



The eSafety Commissioner (eSafety) is Australia's online safety regulator. The Commissioner is an independent statutory authority empowered to help safeguard all Australians from online harms and to promote safer, more positive online experiences. eSafety exercises powers under the Online Safety Act 2021, as well as through sections of the Telecommunications Act 1997 and Criminal Code Act 1995.

eSafety focusses on **protection**, **prevention**, and **proactive and systemic change**. This includes administering user-complaints and investigations schemes, engaging with industry on systemic regulation and promoting online safety through education and research, as well as domestic and international coordination and engagement. Australia has adopted a **hybrid regulatory approach**, targeting harmful material at the user and systems levels. Users are empowered to report harmful material that they encounter under eSafety's four harms schemes: cyberbullying of children, adult cyber abuse, image-based abuse, including NCII, and illegal and restricted content (such as CSAM, TVEC, and criminal activity). eSafety works with users and platforms to have the material removed or blocked. eSafety also has powers to respond to abhorrent violent material, which includes offensive material that is produced by a person who is engaged in or attempts to engage in a terrorist act or other abhorrent violent conduct such as murder, torture, rape and kidnapping.

eSafety's systems-based regulation comprises two frameworks, the Industry Codes and Standards and the Basic Online Safety Expectations (the Expectations). Once all industry codes and standards are in place, they will govern how the online industry is required to deal with illegal content (e.g., CSEA and TVEC) and restricted content (age-inappropriate content such as pornography and high-impact violence).<sup>1</sup> The Expectations outline online safety expectations for social media services, messaging services and communications services including gaming and dating apps, and other internet services such as file-sharing services and websites. The Commissioner can use transparency powers provided in the Online Safety Act to require providers of these online services to report on how they are meeting the Expectations.

## Governing acts and regulation:

[Online Safety Act 2021](#), [Basic Online Safety Expectations](#), [Industry Codes and Standards](#)

Website: [eSafety Commissioner](#)

## Online safety regulatory remit at a glance

Remit and functions	Regulated harms	Regulated entities	Enforcement powers
<ul style="list-style-type: none"> <li>User complaints handling</li> <li>Education and awareness raising</li> <li>Develop, register, and enforce industry regulation (codes and standards)</li> <li>Transparency powers</li> <li>Monitor industry compliance</li> <li>Research</li> <li>Horizon scanning</li> </ul>	<ul style="list-style-type: none"> <li>Cyberbullying of children</li> <li>Adult cyber abuse</li> <li>Image-based abuse</li> <li>Illegal content: includes CSEA material, pro-terror material</li> <li>Restricted content / age-appropriate content</li> </ul>	<ul style="list-style-type: none"> <li>Social media services (SMS) providers</li> <li>Relevant electronic services (RES) providers – includes messaging services and dating apps</li> <li>Designated internet services (DIS) providers – includes file-sharing services, website services, and more</li> <li>Hosting services providers</li> <li>Internet services providers</li> <li>Equipment services providers</li> <li>Search engine services providers</li> <li>App distribution providers</li> </ul>	<ul style="list-style-type: none"> <li>End-user notices</li> <li>Enforceable undertakings</li> <li>Infringement notices</li> <li>Content removal, blocking, and link-deletion</li> <li>Investigations</li> <li>Information gathering</li> <li>Formal warnings</li> <li>Court ordered remedies (E.g. injunctions and civil penalties)</li> <li>Service provider notifications</li> </ul>

<sup>1</sup>The Online Safety Act 2021 (Cth) stipulates that there are eight separate sections of the online industry. The eSafety Commissioner is empowered to register Industry Codes and Standards for each of the eight sections. More information can be found [here](#).



# Fiji: Online Safety Commission (OSC)

The Online Safety Commission (OSC) is Fiji's independent regulator for online safety. The Online Safety Act 2018 was enacted by Parliament of the Republic of Fiji to establish the Online Safety Commission, for the promotion of online safety, deterrence of harmful electronic communication, and other related matters. The OSC started its operations in 2019 to provide an avenue to assist individuals confronted with harmful online content and deliver services and resources to help minimize harm and provide digital literacy, education, and awareness. This includes providing information to Fijian internet users about a variety of current and novel digital platforms, and ways to stay safe online.

The OSC operates a user-complaints scheme that allows users to report harmful content that they encounter online, or harms perpetuated against them or another person online, such as non-consensual sharing of intimate images. The OSC then works with digital services and platforms to have content removed or blocked. At this time, the OSC does not regulate the systems and processes of digital services and platforms.



## Governing acts and regulation:

[Online Safety Act 2018](#), [Online Safety Regulations 2019](#)

Website: [Online Safety Commission](#)

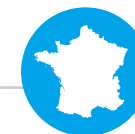
## Online safety regulatory remit at a glance

Remit and functions	Regulated harms	Regulated entities	Enforcement powers
<ul style="list-style-type: none"> <li>User complaints handling</li> <li>Education and awareness raising</li> <li>Receive, assess and investigate matters</li> <li>Horizon scanning</li> </ul>	<ul style="list-style-type: none"> <li>Cyberbullying of children</li> <li>Abuse of adults</li> <li>Image-based abuse</li> <li>Illegal content: includes CSEA material, pro-terror material</li> <li>Restricted content</li> </ul>	<ul style="list-style-type: none"> <li>All platforms and services operating in Fiji that enable 'electronic communication'</li> <li>'Electronic communication' is defined as any form of communication that is transmitted electronically by text, writing, photograph, picture, recording, or any other means</li> </ul>	<ul style="list-style-type: none"> <li>Content removal and blocking orders</li> <li>Financial penalties</li> <li>Investigative powers</li> <li>Information gathering</li> <li>Removal notices</li> </ul>





# France: Arcom



Arcom is the French independent public authority for the regulation of audio-visual and digital communication. Arcom's remit includes many areas, such as spectrum management, broadcasting, video-sharing platforms, and online safety. In these areas, Arcom's missions consist in a technical, economic and legal regulation of the sector, in order to protect freedom of communication in the public interest.

The authority ensures the protection of audio-visual works, combating piracy of cultural and sports content and encouraging the development of legal offers. In addition, Arcom issues authorizations for broadcasting services (TV and radio channels), ensuring pluralism and economic equilibrium in the sector, and is responsible for regulation of on-demand services. It ensures that their programs comply with regulations on the protection of minors, the treatment of information, the organization of election campaigns, advertising, and the representation of society in all its diversity.

In addition to the functions linked to broadcasting regulation in France, Arcom is in charge of supervising the system-based approach of the regulatory framework for online safety that concerns, within the revised AVMS Directive, video-sharing platforms and, within the DSA, categories of intermediary services (such as mere conduit, caching and hosting services, as well as online platforms) that are established in France.

Arcom will be responsible, as Digital Services Coordinators (DSCs), to ensure coordination at national level and supervise enforcement of the DSA with other competent authorities. Within the DSA, intermediary services have to implement tools and resources aimed at combating illegal and harmful content, for the protection of the public in general and more particularly minors, such as reporting and notification mechanisms. Online platforms are also required to empower users with choice and are submitted to transparency requirements for instance. The specific obligations linked to systemic risks on very large platforms (and very large search engines) are exclusively supervised by the European Commission (risk assessments and mitigation measures), in association with Arcom and other competent authorities at the national level in the European Union.

With specific regard to video-sharing platforms, the AVMS Directive adopted in 2010 and revised in 2018 lays down obligations to protect more particularly minors "from programmes, user-created videos and audio-visual commercial communications likely to impair their physical, mental or moral development". In this context, Arcom is responsible for promoting the conclusion of codes of good conduct by video-sharing platforms. Lastly, Arcom is responsible for overseeing the obligations under the system-based approach of the TCO regulation to ensure that platforms effectively implement tools and processes aimed specifically at combatting terrorist content on their services.

## Governing acts and regulation:

[Law n° 86-1067 of 30th September 1986 on freedom of communication;](#)  
[law of June 21st 2004 to support confidence in the digital economy;](#)  
[Directive Audiovisual Media Services \(AVMS\) 2010/13/EU of 10th March \(modified by Directive 2018/1808 of 14 November 2018\);](#) [Regulation 2021/784 of 29 April 2021 on addressing the dissemination of terrorist content online \(TCO\);](#) [Regulation 2022/2065 of 19 October 2022 on a Single Market for Digital Services \(Digital Services Act or DSA\), amending e-commerce Directive \(2000/31/EC\)](#)

Website: [Arcom](#)

## Online safety regulatory remit at a glance

Remit and functions	Regulated harms	Regulated entities	Enforcement powers
<ul style="list-style-type: none"> <li>Education and awareness raising</li> <li>Develop, register, and enforce industry regulation (codes and guidance)</li> <li>Monitor and supervise industry compliance</li> <li>Research</li> <li>Horizon scanning</li> </ul>	<ul style="list-style-type: none"> <li>Illegal content (the circulation of which is an offence under national and EU law)</li> <li>Harmful content: disinformation, promotion of eating disorders</li> <li>Protection of minors: <ul style="list-style-type: none"> <li>content likely to harm their physical, mental or moral development</li> <li>age-appropriate content (access to pornographic sites)</li> <li>commercial use of images of under sixteen children on online platforms</li> </ul> </li> <li>Piracy</li> </ul>	<ul style="list-style-type: none"> <li>Intermediary services: 'mere conduit' services, 'caching' services, 'hosting' services, user-to-user platforms and services and search engine services</li> <li>Video-sharing platforms and services</li> </ul>	<ul style="list-style-type: none"> <li>Investigations</li> <li>Information gathering</li> <li>Formal warnings</li> <li>Financial penalties</li> <li>Apply to a judge for temporary restriction of access to the platform</li> </ul>



# Ireland: Coimisiún na Meán (An Coimisiún)

Coimisiún na Meán is Ireland's agency for developing and regulating a thriving, diverse, creative, safe and trusted media landscape. Its responsibilities are to:

- Oversee the funding of and support the development of the wider media sector in Ireland.
- Oversee the regulation of broadcasting and video-on-demand services.
- Develop and enforce the Irish regulatory regime for online safety (the Online Safety Framework).

The Online Safety Framework is composed of three pieces of legislation:

- The EU Digital Services Act (DSA), for which Coimisiún na Meán has been a competent authority since February 17th 2024.
- The Online Safety Code, derived from the Online Safety and Media Regulation Act. The Code will be adopted and applied in Autumn 2024.
- The EU Terrorist Content Online Regulation (TCOR), for which Coimisiún na Meán has been a competent authority since November 2023.

The Online Safety Framework gives Coimisiún na Meán the tools to address the root causes of harm online, including the availability of illegal content, the harmful impacts of recommender systems, and inadequate protections for children on social media services. An Coimisiún oversees how platforms comply with their online safety obligations at a systemic level and works closely with the European Commission and regulatory counterparts across Europe and beyond. It also carries out research into the areas under its remit and runs media literacy and user education programmes to empower people to critically engage with and understand the media they consume. Coimisiún na Meán also runs an Advice Centre, which gives people information about their rights under the Framework, and escalates issues to a Complaints team for possible supervisory or investigative follow-up.



**Governing acts and regulation:**  
[Broadcasting Act 2009](#) as amended by the [Online Safety and Media Regulation Act 2022](#); [AudioVisual Media Services Directive 2018 \(AVMSD\)](#); [EU Terrorist Content Online Regulation](#); [EU Digital Services Act \(DSA\)](#); [e-Commerce Compliance Strategy](#); [Register of Video Sharing Platforms](#); [Online Safety Code](#)

**Website:** [Coimisiún na Meán](#)

## Online safety regulatory remit at a glance

Remit and functions	Regulated harms	Regulated entities	Enforcement powers
<ul style="list-style-type: none"> <li>• Education and awareness raising</li> <li>• Develop, register, and enforce industry regulation (codes and guidance)</li> <li>• Monitor and supervise industry compliance</li> <li>• Research</li> <li>• Horizon scanning</li> </ul>	<ul style="list-style-type: none"> <li>• Illegal content</li> <li>• CSAM</li> <li>• Terrorism</li> <li>• Harmful content including pornography and extreme or gratuitous violence</li> <li>• Promotion of self harm or suicide</li> <li>• Promotion of eating or feeding disorders</li> <li>• Cyberbullying</li> <li>• Dangerous challenges</li> <li>• Incitement to hatred or violence on grounds of protected characteristics including racism and xenophobia</li> <li>• Harmful or illegal commercial communications</li> </ul>	<ul style="list-style-type: none"> <li>• Video-sharing platforms and services</li> <li>• Intermediary services: 'mere conduit' services, 'caching' services, 'hosting' services, platforms and services and search engine services</li> <li>• Hosting Services Providers exposed to Terrorist Content online</li> </ul>	<ul style="list-style-type: none"> <li>• Investigations</li> <li>• Financial sanctions</li> <li>• Auditing</li> <li>• Content Limitation Notices</li> <li>• Access Blocking Orders</li> <li>• Compliance notices</li> <li>• Criminal powers</li> </ul>



# Republic of Korea: Korea Communications and Standards Commission (KCSC)



Korea Communications Standards Commission (KCSC) is an independent statutory body responsible for regulating media content in the Republic of Korea. Established in 2008 under the Act on the Establishment and Operation of the Korea Communications Commission, it was formed by merging the Korea Internet Safety Commission and the regulatory function of the Korea Broadcasting Commission.

The KCSC comprises nine Commissioners appointed by the President of Korea. Article 18 (Establishment of KCSC, etc) of the aforementioned act outlines the appointment process, where three Commissioners are appointed by the Speaker of the National Assembly in consultation with representatives from each negotiation party, and three are appointed by the Standing Committees of the National Assembly. Each Commissioner serves a three-year term with the possibility of one re-election. There are three Standing Commissioners including the chairperson, who is elected from among the nine Commissioners. The secretariat is composed of the secretary general, two offices (Audit Office, Planning and Coordination Office), four bureaus (Broadcasting Content Review Bureau, Internet Communications Content Review Bureau, Rights Protection Bureau, Digital Sex Crime Content Review Bureau), one group (International Cooperation Group), one center (Center for Policy Research), twenty-seven divisions, and five regional offices in Busan, Gwangju, Daegu, Daejeon, and Gangwon-do. As of today, the KCSC employed 204 staff members.

The duties of the KCSC, as outlined in Article 21 (Duties of the Korea Communications Standards Commission) of the aforementioned act, encompass the review of TV broadcasting content, TV advertisements, and internet communications content. To ensure responsiveness to the rapidly evolving media landscape and strengthen the review system and relevant regulatory framework, the KCSC establishes, announces, and amends its review principles and content standards. The KCSC also engages in research, promotes public campaigns, and hosts educational programs and seminars to enhance media literacy and ethics. With the June 2021 amendment, the KCSC took on the added role of international cooperation to cultivate a safe online environment that is both healthy and trusted by the public, in partnership with global counterparts.

To maximize the efficiency of the KCSC's dealings, the KCSC conducts various meetings including the Standing Commission, General Meeting, four Sub-commission, five Special Advisory Committees, Defamation Disputes Mediation Committee, and Election Broadcasting Review Committee.

## Governing acts and regulation:

[Act on the Establishment and Operation of the Korea Communications Commission; Act on Promotion of Information and Communications Network Utilization and Information Protection; Telecommunications Business Act](#)

**Website:** [Korea Communications and Standards Commission](#)

## Online safety regulatory remit at a glance

Remit and functions	Regulated harms	Regulated entities	Enforcement powers
<ul style="list-style-type: none"> <li>Education and awareness raising</li> <li>Develop, register, and enforce industry regulation (codes and guidance)</li> <li>Monitor and supervise industry compliance</li> <li>Research</li> <li>Horizon scanning</li> </ul>	<ul style="list-style-type: none"> <li>Illegal harms: Includes gambling, privacy violations, illegal financial activities, fraud, illegal sales of food, drugs, and narcotics, trade of sperm, eggs, and organs, violations of the National Security Act, pro-terrorism content, pornography, CSAM, CSEM, NCII, human trafficking, and other content that violates legal order</li> <li>Content Legal but Harmful to Children: Includes content that promotes eating disorders, cruel or hateful content, content that discriminates against or demeans specific groups, content that causes social disorder, and illegal or harmful content within webcasting</li> <li>Defamation and Privacy Violations: Includes defamation, invasion of privacy and personal freedoms, infringement of portrait rights</li> </ul>	<ul style="list-style-type: none"> <li>Information and communications service providers refer to entities that either operate as telecommunications business operators or use the services of these operators to provide or facilitate the provision of content for profit. This includes platforms and services that deliver content to the public or act as intermediaries in content distribution using telecommunications networks</li> <li>Internet bulletin board administrators and operators</li> </ul>	<ul style="list-style-type: none"> <li>Content removal</li> <li>Access blocking</li> <li>User account cancellation/suspension</li> <li>Financial penalties</li> <li>Investigations</li> <li>Information requests</li> <li>Infringement notices</li> <li>End-user notices</li> <li>Platform/Service Provider notifications</li> </ul>



# Slovakia: Council for Media Services (CMS)



Council for Media Services (CMS) is Slovakia's independent media regulator responsible for media oversight and enforcement of regulatory frameworks pertinent to broadcasting, retransmission, provision of on-demand audiovisual media services, and digital platforms. The mission of CMS is to protect the public online as well as to enforce the public interest in the exercise of the right to information, freedom of expression, and the right of access to cultural values and education. CMS is a leading member of the European Regulators Group for Audiovisual Media Services (ERGA), European Platform of Regulatory Authorities (EPRA), and the DSA Board.

CMS was established in 2022 by the Media Services Act (MSA), replacing Council for Broadcasting and Retransmission, a national regulatory authority supervising primarily the linear media market. Taking into consideration the legislative developments on the EU level, the Media Services Act transposed the Audio-Visual Media Services Directive (AVMSD), implemented EU Regulation addressing the dissemination of terrorist content online (TCO) and began preparations for the adoption of the Digital Services Act (DSA). Traditionally, CMS has overseen the establishment (e.g. authorization, registration, issuance of licenses) and conduct of broadcasters in Slovakia. However, the MSA has introduced new obligations, namely requirements related to the provision and conduct of audio-visual media services (including vloggers), European works, independent production and assessment of measures taken by video-sharing platforms (VSPs) to protect the public. In light of the latter, the MSA also empowers CMS to address online safety risks arising from the functioning and design of online platforms.

As part of its online safety remit, CMS is tasked with overseeing the effectiveness and proportionality of the enforcement of terms of service of online platforms offering their services in Slovakia. Moreover, CMS has the legal competence to tackle the dissemination of illegal content online by issuing content removal orders for content that violates art. 151 of the MSA. CMS also engages in research, media literacy and international cooperation.

As a Digital Services Coordinator (DSC), CMS is responsible for all DSA provisions, and thus oversees the conduct and functioning of the online platforms established in Slovakia.

## Governing acts and regulation:

[the Media Services Act \(MSA\); Directive Audiovisual Media Services \(AVMS\) 2010/13/EU of 10th March \(modified by Directive 2018/1808 of 14 November 2018\); Regulation 2021/784 of 29 April 2021 on addressing the dissemination of terrorist content online \(TCO\); Regulation 2022/2065 of 19 October 2022 on a Single Market for Digital Services \(Digital Services Act or DSA\), amending e-commerce Directive \(2000/31/EC\)](#)

Website: [Council for Media Services](#)

## Online safety regulatory remit at a glance

Remit and functions	Regulated harms	Regulated entities	Enforcement powers
<ul style="list-style-type: none"> <li>User complaints handling</li> <li>Develop, register and enforce industry regulation (self/co-regulatory mechanisms, codes and guidance)</li> <li>Monitor and supervise industry compliance</li> <li>Research</li> <li>Education and awareness raising</li> <li>Horizon scanning</li> </ul>	<ul style="list-style-type: none"> <li>Illegal content (content depicting CSEA or extremism; content inciting to violence or featuring acts of terrorism; content approving or praising acts of terrorism; content denying or approving the Holocaust, crimes of political regimes, crimes against humanity, defamation of a nation, race and belief, or incitement to national, racial and ethnic hatred)</li> <li>Protection of minors</li> <li>Harmful content covered by platforms' ToS (disinformation, scams, etc.)</li> </ul>	<ul style="list-style-type: none"> <li>Audio-Visual Media Services Providers</li> <li>Intermediary services: mere conduit, caching, hosting, platforms, marketplaces, search engines</li> <li>Video-sharing platforms</li> </ul>	<ul style="list-style-type: none"> <li>Investigations</li> <li>On-site inspections and interviews</li> <li>Requests for information</li> <li>Formal warnings</li> <li>Content removal orders</li> <li>Court-ordered remedies</li> <li>Financial penalties</li> <li>Requests to adopt an action plan</li> </ul>



# South Africa: Film and Publications Board (FPB)



The Film and Publication Board (FPB) is a state entity established under the Films and Publications Act (FPA) 1996, as amended. The FPB has a broad remit and regulates the creation, possession and distribution of films, games, certain publications, and digital content on platforms and services. The regulation seeks to protect children from disturbing and harmful content and to provide content information to adults that will enable them to make informed reading, viewing and gaming choices for both themselves and children in their care.

South Africa has adopted a **hybrid approach** to online safety regulation, developing industry codes of practice and operating a user-complaints scheme. The FPA empowers the FPB to issue directives of general application. The FPB has also developed an advisory industry code on prevention of online harm. Under FPB's user complaints scheme, users can report harmful content such as CSAM, filming and distribution of films and photographs depicting violence against children, hate speech, distribution of private sexual photographs and films, incitement of imminent violence and propaganda for war.

## Governing acts and regulation:

[Films and Publications Act 65 of 1996](#)  
[Film and Publications Amendment Regulations 2022](#)

Website: [Film and Publication Board](#)

## Online safety regulatory remit at a glance

Remit and functions	Regulated harms	Regulated entities	Enforcement powers
<ul style="list-style-type: none"> <li>• Education and awareness raising</li> <li>• Develop industry regulation and guidance</li> <li>• Monitor and supervise industry compliance</li> <li>• Research</li> <li>• Horizon scanning</li> </ul>	<ul style="list-style-type: none"> <li>• CSAM</li> <li>• Filming and distribution of films and photograph depicting sexual violence and violence against children</li> <li>• Unclassified content</li> <li>• Harmful and prohibited content</li> <li>• Online hate speech</li> <li>• Propaganda for war</li> <li>• Incitement of imminent violence</li> <li>• Distribution of private sexual photographs and films</li> </ul>	<ul style="list-style-type: none"> <li>• Commercial online distributors of films, games and certain publications</li> <li>• Video-sharing platforms and services</li> <li>• User-to-user platforms and services</li> <li>• Search engine services</li> <li>• Internet Service and Access Service Providers</li> </ul>	<ul style="list-style-type: none"> <li>• Investigations</li> <li>• Compliance notice</li> <li>• Take down notices</li> <li>• Adjudication of non-compliance by the Enforcement Committee with powers to impose fines</li> <li>• Referral for criminal prosecution</li> </ul>



# United Kingdom: Ofcom

Ofcom is the UK's communications regulator. Ofcom's remit covers a wide range of areas, including spectrum, post, telecommunications networks, broadcasting, video-sharing platforms, and online safety. Following the passing of the Online Safety Act in October 2023, Ofcom took on broader online safety duties, including the regulation of user-to-user and search services accessed by UK users.

The UK has adopted a **systems and processes based approach** to online safety regulation under the Online Safety Act, that will require services to undertake risk assessments and adopt content safeguards. Some services will be subject to additional obligations, including empowering users with choice and publishing transparency reports. Ofcom is taking a phased approach to implementation and by mid-2026, Ofcom aims to have developed and finalised Codes of Practice and Guidance to recommend ways in which services can comply with their obligations under the Online Safety Act. Ofcom also undertakes research into online safety and delivers media literacy education and awareness raising.



**Governing acts and regulation:**

[Online Safety Act 2023](#)

**Website:** [Ofcom](#)

## Online safety regulatory remit at a glance

Remit and functions	Regulated harms	Regulated entities	Enforcement powers
<ul style="list-style-type: none"> <li>Enforce legal duties</li> <li>Develop non-binding industry regulation (codes and guidance)</li> <li>Monitor and supervise industry compliance</li> <li>Research</li> <li>Horizon scanning</li> <li>Education and awareness raising</li> </ul>	<ul style="list-style-type: none"> <li>Illegal content (such as CSAM, terrorism, fraud, drug offences, and human trafficking, among others)</li> <li>Content that is legal but harmful to children (such as pornography, promotion of self-harm, suicide, and eating disorders, bullying content, among others)</li> </ul>	<ul style="list-style-type: none"> <li>User-to-user platforms and services</li> <li>Search engine services</li> <li>Providers publishing pornographic content</li> </ul>	<ul style="list-style-type: none"> <li>Investigations</li> <li>Information gathering</li> <li>Court ordered remedies (e.g. business disruption measures and injunctions)</li> <li>Financial penalties</li> <li>Criminal sanctions</li> </ul>





# Regulatory analyses

- Online safety regulatory remits
- Online harms
- Regulated entities
- Obligations for regulated entities
- Information gathering and enforcement



# Online safety regulatory remits

There are similarities between regulatory remits and functions of regulators. Regulatory remits and functions typically vary in relation to the foundational approach, namely whether the jurisdiction has adopted a **content-based**, **systems-based**, or **hybrid approach**. Content-based regulatory models seek to address harmful content by providing complaints and redress for users who are experiencing or have encountered harmful content. Systems-based regulation focuses on imposing requirements upon the design and operation of digital platforms and services to mitigate risks that may exist on their service through inbuilt safety interventions.

As demonstrated, all member regulators are authorised to carry out varying enforcement actions and all undertake online safety education and awareness raising. Most undertake research and have the capacity to receive and investigate complaints from users. Further, most regulators are provided with the authority to develop and enforce industry codes of practice.

The table below captures the online safety remits of regulators. It is worth noting that some regulators have broad remits that extend beyond online safety (e.g. classifications of films, broadcasting, and media regulation).

Jurisdiction	Regulatory remits and functions												
	Ex ante regulation	User complaints and investigations					Information gathering and enforcement			Prevention research and engagement			
	Develop and enforce codes, standards, and guidance	Proactive content scanning <sup>2</sup>	Receive and investigate individual user complaints	Issue content removal and blocking notices	Partnership with law enforcement and hotline networks	Service blocking or restriction orders (e.g., service, access, or payment blocking orders)	Oversight and transparency	Non-compliance notices and financial penalties	Court orders and injunctions	Education and awareness raising	Grants	Research and horizon scanning	Industry engagement
Australia (eSafety)	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Fiji (OSC)	✗	✗	✓	✓	✓	✗	✗	✓	✓	✓	✗	✗ <sup>3</sup>	✓
France (Arcom)	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓
Ireland (An Coimisiún)	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓
Republic of Korea (KCSC)	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓
Slovakia (CMS)	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗	✓	✓
South Africa (FPB)	✓ <sup>4</sup>	✓	✓	✓	✓	✗	✓	✓	✓	✓	✗	✓	✓
United Kingdom (Ofcom)	✓ <sup>5</sup>	✗	✗	✗	✗ <sup>6</sup>	✓	✓	✓	✓	✓	✗	✓	✓

<sup>2</sup>In this context, proactive content scanning refers to content scanning carried out by the regulator. Some regulators may require regulated entities to undertake proactive content scanning in certain circumstances. <sup>3</sup>Fiji OSC online does perform horizon scanning functions, but does not have a research function. <sup>4</sup>The Film and Publications Board has authority to develop codes and guidance. However the FPB does not presently have the authority to enforce codes and guidance. <sup>5</sup>In the UK, Ofcom can enforce legal duties (derived from legislation) and can develop non-binding codes and guidance. <sup>6</sup>However, Ofcom engages with law enforcement and hotline networks.





# Regulated online harms

There are some limitations associated with comparing the online harms regulated by each jurisdiction, as definitions of harms are complex and not always ‘like for like.’ Though all jurisdictions regulate categories of ‘illegal harms’ and ‘content that is harmful to youth,’ the legal definition of each category of harm varies between jurisdictions. For example, what is considered as **‘illegal content’** varies from country to country and is generally determined by the criminal laws or classification framework of that country. Within most member jurisdictions, illegal content includes CSAM, terrorism and extremism (TVEC), the depiction, promotion, or incitement of violence (including murder, assault, rape, etc), sexual exploitation, and content that depicts, promotes or attempts to sell illegal substances or weapons. However, we note that in some jurisdictions, abusive content, ‘illegal hate speech,’ defamation, and pornography are also considered illegal.

‘**Harmful content**’ also referred to as ‘**restricted content**’ or ‘**age-inappropriate content**,’ also varies significantly between jurisdictions, as national thresholds differ in relation to what is considered ‘potentially harmful to the physical, psychological, and developmental wellbeing of children.’ For example, pornography is considered illegal in some jurisdictions and ‘restricted’ in others.

Furthermore, in several jurisdictions there is some overlap between categories of harmful content. For example, in some contexts, the category ‘**abuse and harassment**’ covers most examples of ‘**online hate and discrimination**.’ In some contexts, ‘hate speech’ is narrow and refers only to language, whereas other jurisdictions use the broader terminology ‘online hate’ to also refer to hateful imagery, video, and symbols. It is also worth noting that regulatory powers and obligations for regulated entities do not apply in equal force across all categories of online harms and also vary between jurisdictions. Generally, the most severe harms (those that are illegal in all jurisdictions) such as CSEM, CSAM, and TVEC, attract the most stringent regulatory requirements.

Jurisdiction	Online harm types															
	CSEM / CSAM	TVEC / Pro-Terror	Hate speech and discrimination	Illegal content	Fraud and financial harms	Incitement and depictions of violence	Misinformation and disinformation	Image-based abuse Non-consensual sharing of intimate images	Cyberbullying of children	Abuse and harassment	Promotion of dangerous conduct (e.g., eating disorders, self-harm, suicide, dangerous activities, etc)	Harmful algorithmic patterns	Defamation	Content against national interests	Pornography	
Australia (eSafety)	✓	✓	✗ <sup>7</sup>	✓	✗	✓	✗ <sup>8</sup>	✓	✓	✓	✗	✗	✗	✗	✓	
Fiji (OSC)	✓	✓	✗	✓	✗	✓	✗	✓	✓	✓	✗	✗	✗	✗	✓	
France (Arcom)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	
Ireland (An Coimisiún)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗ <sup>9</sup>	✗	✓	
Republic of Korea (KCSC)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Slovakia (CMS)	✓	✓	✓	✓	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	
South Africa (FPB)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗	✗	✓	
United Kingdom (Ofcom)	✓	✓	✓	✓	✓	✓	✗ <sup>10</sup>	✓	✓	✓	✓	✓	✗	✗	✓	

<sup>7</sup>The eSafety Commissioner only regulates online hate and defamation that meets the threshold for adult cyber abuse or cyberbullying of children. Under eSafety’s transparency framework (the Expectations), platforms and services may be required to provide information about their efforts to tackle a wide range of online harms, including online hate, dangerous challenges, content that promotes suicide and self harm, and harmful algorithmic patterns. Australia has separate criminal and civil laws that deal with certain forms of hate speech and discrimination. <sup>8</sup>Australia is currently progressing legislation on misinformation and disinformation, and the Australian Communications and Media Authority administers a voluntary code of practice on misinformation and disinformation. <sup>9</sup>Unless related to reporting of illegal content removal orders under the DSA. <sup>10</sup>Some forms of misinformation and disinformation may be caught if they fall under scope of the UK’s foreign interference and false communications offences.

# Regulated entities

Analysis of the types of entities regulated in each jurisdiction is complex and does not lend itself to simple comparison as there are many definitional challenges. For example, there is significant overlap between the categories of **social media services, video-sharing platforms and services**, and **user-to-user platforms and services**. In the UK and EU, video-sharing platforms and services (VSPs), such as YouTube and TikTok, are a distinct category of regulated entity, in recognition of the risks associated with user-to-user video virality. Conversely, 'VSP' is not a legally defined category of regulated entities in Australia and the Republic of Korea. Instead platforms like YouTube, TikTok, and others with video-sharing functionalities, are captured under the definition of 'social media service.' So, where some jurisdictions choose to separate out sections of the online industry, others choose to combine into larger categories.

Similarly, **'user-to-user services' (U2U)** such as messaging apps, dating apps, games with communication functionalities, and other social media platforms are not a standalone category of 'regulated entities' in all jurisdictions. Some jurisdictions, like Australia and the Republic of Korea capture U2U services across other categories of entities such 'social media services' or 'messaging services.' What is important to note is that all jurisdictions capture the large mainstream online platforms and services in some way.

Jurisdiction	Categories of digital services and platforms										
	Social media services, Video-sharing platforms and services, User-to-user platforms and services	Hosting and storage services	Gaming services	App distribution services	Internet service providers	Messaging services and dating apps	End-to-end encrypted services	Search engine services	Websites	Generative AI services	Equipment services
Australia (eSafety)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Fiji (OSC)	✓	✗	✓	✗	✗	✓	✓	✓	✗	✗	✗
France (Arcom)	✓	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗
Ireland (An Coimisiún)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗
Republic of Korea (KCSC)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓ <sup>12</sup>	✓
Slovakia (CMS)	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗
South Africa (FPB)	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗
United Kingdom (Ofcom) <sup>11</sup>	✓	✓	✓	✗	✗	✓	✓	✓	✓	✓	✗

<sup>11</sup>In the UK, only services that are user-to-user, search or online pornography services are regulated entities under the Online Safety Act (2023). All categories marked as 'YES' are to the extent that are user-to-user, search or online pornography services. <sup>12</sup>KCSC regulates content on platforms like DALL-E because its content is publicly accessible. However, services such as ChatGPT are not regulated by KCSC because it interacts privately with individual users.



# Obligations for regulated entities

Analysis of obligations for regulated entities is complex and does not lend itself to simple comparison. This is because regulatory obligations and requirements do not necessarily apply equally across all categories of regulated online harms and regulated entities. Adding to the complexity, there is significant variation in how regulation applies within a single category of regulated entities, with most jurisdictions adopting a risk-based approach (or ‘tiered’ approach) to regulate in a way that is proportionate to the risks that exist on a particular platform or service. Most jurisdictions have imposed stricter and more onerous requirements on larger, riskier platforms.

Each jurisdiction varies in how it assesses or categorises ‘risk’ within their regulatory framework, with most taking into account a combination of factors such as number of users, user-demographics, geographical spread, service functionalities, type and number of content risks, likelihood and impact of online harms, service purpose, discoverability, algorithms and recommender usage, and more. The table below serves as a foundation of comparison, providing a broad overview of the types of interventions and requirements imposed by regulators across member jurisdictions.

Jurisdiction	Obligations for regulated entities																	
	Designate domestic agent able to receive legal notices	Comply with content removal, blocking, and link deletion notices	Comply with timeliness requirements for content notices	Comply with registered codes and standards	Adequately respond to information requests	Comply with transparency reporting and oversight requirements	Undertake risk assessments	Establish appropriate governance	Record keeping	Submit to auditing as required	Proactively minimise harmful and unlawful content	Empower users with choice	Implement age-assurance systems	Take reasonable steps to protect children from content that is not age-appropriate	Take reasonable steps to ensure E2EE and anonymous services are safe	Provide user reporting mechanisms	Provide and enforce clear and accessible terms of service	Undertake online safety professional education
Australia (eSafety)	✗ <sup>13</sup>	✓	✓	✓	✓	✓	✓ <sup>14</sup>	✓	✓	✗	✓	✓ <sup>15</sup>	✗	✓	✓	✓	✓	✗
Fiji (OSC)	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗
France (Arcom)	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗
Ireland (An Coimisiún)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Republic of Korea (KCSC)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Slovakia (CMS)	✓ <sup>16</sup>	✓	✓	✓	✓	✓	✗	✗	✓	✗	✗	✓	✗	✓	✗	✓	✓	✗
South Africa (FPB)	✓	✓	✓	✓	✓	✗	✓	✗	✗	✗	✓	✗	✗	✓	✗	✓	✗	✗
United Kingdom (Ofcom)	✗	✗	✗	✓ <sup>17</sup>	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗

<sup>13</sup>Under Australia’s transparency framework (the Expectations), some platforms and services are expected to designate a legal point of contact. This does not need to be located domestically. <sup>14</sup>Under Australia’s online safety framework, platforms and services are only required to undertake risk assessments, provide clear and accessible Terms of Service, and provide user reporting mechanisms in relation to class 1 material. Class 1 material includes CSAM, pro-terror material, and criminal material such as violence and drug-related content. <sup>15</sup>In Australia, some platforms and services such as messaging services are required to provide choice to users such as account blocking features. Under The Expectations, platforms and services may be required to provide information on their efforts to empower users with the ability to personalise their online experience. <sup>16</sup>Under the DSA, CMS may require a regulated entity to designate a domestic agent capable of receiving legal notices only if the regulated entity is headquartered in Slovakia. <sup>17</sup>In the UK, regulated entities are required to comply with duties set out in the Online Safety Act (2023). Ofcom issues codes which recommend steps that regulated entities can take to comply.

# Information gathering and enforcement

Most jurisdictions adopt similar approaches to information gathering and enforcement, consisting of powers to obtain information through notices and supervisory functions, and firmer powers such as financial penalties or court ordered remedies. Importantly, not all enforcement powers are available in all instances of non-compliance. For some regulators, firmer powers such as business disruption orders and civil penalties only become available after recurring non-compliance with information requests. Other regulators are able to issue financial penalties in instances where content removal deadlines are breached. Further, the quantum of financial and civil penalties varies significantly between jurisdictions, with some able to issue fines of up to 10 per cent of global annual revenue. Noting those nuances, the table below provides a general overview of the various enforcement mechanisms available in each jurisdiction.

Jurisdiction	Information gathering and enforcement															
	Content-based enforcement actions				Information gathering powers						Systems-based regulatory enforcement		Court ordered remedies			
	Formal written warning	Take-down, deletion, and blocking notices	Actor or account-level directives <sup>18</sup>	Financial penalties	Information notices	Supervisory powers	Transparency reporting requirements	Third party auditing	Submit to interview	Power of entry, inspection and audit	Formal written warnings and remedial directions (e.g., undertakings)	Financial penalties	Civil and administrative penalties	Injunctions	Service blocking or restriction orders (e.g., service, access, or payment blocking orders) <sup>19</sup>	Damages
Australia (eSafety)	✓	✓	✓	✓	✓	✗	✓	✗	✓	✗	✓	✓	✓	✓	✓	✗
Fiji (OSC)	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✗	✓
France (Arcom)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	✓
Ireland (An Coimisiún)	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Republic of Korea (KCSC)	✓	✓	✓	✓	✓	✗	✗	✓	✓	✗	✓	✓	✓	✓	✓	✓
Slovakia (CMS)	✓	✓	✗	✓	✓	✓	✓	✗	✓	✓	✓	✓	✗	✗	✗	✗
South Africa (FPB)	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✗	✓	✓	✓	✗	✓
United Kingdom (Ofcom)	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓

<sup>18</sup>'Account or actor-level directives' refer to directives or notices issued to end-users or platforms to facilitate removal of an account or individual from the specified platform or service. <sup>19</sup>Service blocking and restriction orders includes 'business disruption orders.'