# Online Safety: a comparison of key UK, EU, Singapore and UAE legislation

ReedSmith

This table sets out a comparison between the European Union Digital Services Act (DSA), the UK's Online Safety Act (OSA), the European Union Digital Markets Act (DMA), the UAE Child Digital Safety Law and the Singapore Broadcasting Act as of March 2026.

| | DIGITAL SERVICES ACT (EU) | ONLINE SAFETY ACT (UK) | DIGITAL MARKETS ACT (EU) | BROADCASTING ACT (SG) | Child Digital Safety Law (UAE) |
|---|---|---|---|---|---|
| | **Scope** | | | | |
| **Whom it applies to** | **"Online intermediary services". Intermediary services cover services which cache or host third-party content or act as a mere conduit. There are tiered obligations which differ depending on the type of service, with key categories being as follows:**<br><br>• Hosting services: platforms which store information provided by the recipient of the service.<br><br>• Online platforms: a sub-set of hosting providers being platforms bringing together sellers and consumers, such as online marketplaces, app stores, collaborative economy platforms, and social media platforms. Exempted from this classification are ancillary features (e.g. comments against newspaper articles) and private messaging.<br><br>• Very large online platforms (VLOPs): platforms with more than 10% of the 450 million monthly active users in the EU.<br><br>• Very large search engines (VLOSEs) with more than 10% of the 450 million consumers in EU.<br><br>Micro and small companies have obligations proportionate to their ability and size while ensuring they remain accountable. In addition, even if micro and small companies grow significantly, they would benefit from a targeted exemption from a set of obligations during a transitional 12-month period. | **Services that provide online user interactions and user-generated content (user-to-user services) and search services with links to the UK (including where the provider is located outside the UK).**<br><br>• Services covered include social media platforms, consumer cloud storage sites, video-sharing platforms, online forums, gaming sites, online marketplaces, and search engines.<br><br>• Providers will be classified into Category 1, Category 2(A), and Category 2(B), with Category 1 companies being those considered as "high-risk and high-reach."<br><br>• There are certain separate duties that apply specifically to internet services that display or publish pornographic content.<br><br>Exemptions include providers of certain communication services (e.g. providers of emails, SMS, MMS services, or combination of such services), services with limited functionality (e.g. where the only user-generated content are comments or reviews relating to provider's content), internal business services, services provided by public bodies and providers of education or childcare. | **Platforms acting as digital "gatekeepers" to the single market**<br><br>A platform qualifies as a gatekeeper if it operates a "core platform service" whereby:<br><br>• It either has had an annual turnover of at least €7.5 billion within the EU in the past three years, or has a market valuation of at least €75 billion;<br><br>• It has at least 45 million monthly end users and at least 10,000 business users in the EU.<br><br>"Core platform services" include web browser and voice assistants, among others, but excludes connected TVs. The key is that a gatekeeper provides access to other third-party services and offers.<br><br>Small and medium-sized enterprises are exempt from being gatekeepers, apart from in exceptional cases. However, there is a category of "emerging gatekeepers," meaning that the European Commission (the Commission) can impose obligations on companies whose competitive position is proven but not yet sustainable.<br><br>The European Commission announced companies it considers to be gatekeepers **here** on September 6, 2023. | **Online communication services that have "significant reach or impact"**<br><br>An online communication service is covered if it has significant reach or impact. This includes electronic services with the following characteristics:<br><br>**a.** The sole or primary purpose of the service is to enable online interaction or linking between two or more end users (including enabling end users to share content for social purposes);<br><br>**b.** The service allows end users to communicate content on the service; and<br><br>**c.** Any other characteristics prescribed by Infocomm Media Development Authority (IMDA) regulations.<br><br>For now, only social media services are regulated online communication services, except for communications of a private or domestic nature. This can be varied in the future by the IMDA. | **Internet service providers (ISPs), Digital Platforms (defined as: "The electronic means that enables interaction and communication among users in the digital space and provides digital services or content") and Caregivers (i.e. Persons legally responsible for children (under 18s) whether a parent, guardian, or any person entrusted under the law with the child's care and with making decisions relating to the child's protection and safety).**<br><br>The Child Digital Safety Law applies wherever children use Digital Platforms or are exposed to the Digital Platform's contents or services.<br><br>Digital Platforms include, but are not limited to, the following:<br><br>**a.** Websites<br><br>**b.** Electronic search engines<br><br>**c.** Smart applications, messaging apps, and forums<br><br>**d.** Electronic games platforms<br><br>**e.** Social media platforms<br><br>**f.** Live streaming platforms<br><br>**g.** Podcast platforms<br><br>**h.** Streaming services and on-demand online video content platforms<br><br>**i.** E-commerce platforms<br><br>Each of ISPs, Digital Platforms and Caregivers are subject to separate obligations under the Child Digital Safety Law and the specific obligations applicable to different types of Digital Platforms are to be set out under a separate decision. |

| | DIGITAL SERVICES ACT (EU) | ONLINE SAFETY ACT (UK) | DIGITAL MARKETS ACT (EU) | BROADCASTING ACT (SG) | Child Digital Safety Law (UAE) |
|---|---|---|---|---|---|
| **Territorial scope** | **Online intermediary services offering their services in the EU.** | **Service with links to the UK**<br><br>A service has links to the UK if:<br><br>• It has a significant number of UK users; or<br><br>• UK users form one or the only target market for the service; or<br><br>• It is capable of being used in the UK by individuals and there are reasonable grounds to believe that there is a material risk of significant harm to individuals in the UK from content present (user-to-user services) or content that might be encountered in or via search results (search services). | **Platforms offering their services in the EU and controlling one or more core platform services (such as browsers, messengers, or social media) in at least three member states.** | **Service with links to Singapore.**<br><br>A service has links to Singapore if:<br><br>• The service is between a point in Singapore and one or more other points in Singapore; or<br><br>• The service is between a point outside Singapore and at least one point in Singapore. | **Wherever a Digital Platform operates within the UAE or targets users in the UAE.**<br><br>Whilst the Child Digital Safety Law does not set out specific factors which constitute targeting, there are various factors which, if present, may indicate that the UAE market is being targeted, including (by way of indication only):<br><br>• localised, UAE specific content on the website or platform;<br><br>• advertising which specifically targets UAE based users. Physical advertisements in the UAE (e.g. Billboards) or UAE specific online advertising (e.g. Advertising copy which expressly references the UAE, uses imagery relating to the UAE or references pricing in local currency (AED Dirhams));<br><br>• display of prices in local currency (UAE Dirhams). |
| **What type of content is covered?** | **Illegal content.**<br><br>• Illegal content covering information that, in itself or in relation to an activity, including the sale of products or the provision of services, is not in compliance with Union law or the law of a member state that is in compliance with Union law, irrespective of the precise subject matter or nature of that law. | **Illegal content and content harmful to children.**<br><br>• Content (for the purposes of defining a user-to-user service) covers any content communicated by means of an internet service whether publicly or privately including written material or messages, oral communications, photos, videos, visual images, music and data of any description.<br><br>• Illegal content means content that (including the dissemination, possession, or accessing of which) amounts to a relevant offence. Illegal content falls into the category of "priority illegal content" if it is terrorism content, CESA content or content that amounts to an offence covered in Schedule 7 to the OSA.<br><br>• Content is harmful to minors if it is primary priority content that is harmful to minors (covers various listed content including pornographic content, content that encourages, promotes or provides instructions for suicide or for an act of deliberate self-injury or for an eating disorder or behaviors associated with an eating disorder); or priority content that is harmful to minors (abusive content that targets specific listed characteristics including race, religion, sexual orientation and gender reassignment, which incites hatred, bullying content, depictions of real or realistic serious violence against a person or animal, encourages or promotes instructions for a challenge or stunt highly likely to result in serious injury, etc). | **Not directly covered.** | **"Egregious" content, including content that may otherwise be legal.**<br><br>• Egregious content means content that advocates or instructs on:<br><br>  • Suicide or self-harm;<br><br>  • Violence or cruelty or other infliction of serious physical harm on human beings;<br><br>  • Sexual violence, depicting child nudity for a sexual purpose, or exploiting child nudity in an offensive way;<br><br>  • Conduct that is likely to obstruct public health measures or result in a public health risk in Singapore;<br><br>  • Dealing with race or religion in a way that is likely to cause ill will, contempt, or ridicule other racial or religious groups in Singapore; or<br><br>  • Terrorism and any other content prescribed by IMDA regulations.<br><br>• Whether the content is conducted within or outside Singapore is immaterial.<br><br>For now, the legislation does not cover infliction of serious physical harm on living things other than human beings, even if these acts are illegal, or communications of a private or domestic nature. | **All content on the Digital Platform**<br><br>There are specific restrictions with respect to "Harmful Content" and "Child Pornography".<br><br>Harmful Content covers various types of content which are likely to negatively affect the moral, psychological, or social values of children or society, and that violate media content standards. The media content standards are set out under various other laws and regulations which apply concurrently including, without limitation, the overarching Federal Media Law and its implementing regulations.<br><br>Child Pornography covers images, videos and illustrations which are published, displayed, or circulated via any communication means, social media networks, or other electronic or virtual platforms, in which a child is depicted engaging in sexual acts or sexual exhibition, whether real, fictional, or simulated, or through any representation of the child's sexual organs for sexual purposes. |

| | DIGITAL SERVICES ACT (EU) | ONLINE SAFETY ACT (UK) | DIGITAL MARKETS ACT (EU) | BROADCASTING ACT (SG) | Child Digital Safety Law (UAE) |
|---|---|---|---|---|---|
| **Protection of minors** | **Obligations for the protection of minors are included.**<br>• Online platforms are required to have appropriate and proportionate measures to ensure a high level of privacy, safety, and security for minors. The European Commission has published guidelines on its expectations **here**.<br>• VLOPs need to have reasonable, proportionate, and effective mitigation measures (tailored to risks), which may include age verification.<br>• Bans on targeted advertisements to minors based on profiling of their personal data.<br>• All intermediary services primarily directed at minors or predominantly used by minors should make particular effort to render the exploitations of their terms and conditions easily understandable to minors.<br>• Additional obligations on VLOPs and VLOSEs to protect minors, including assessments.<br>• Note: "minors" means an individual under the age of 18. | **Specific duties if services are likely to be accessed by minors.**<br>• Services have to carry out a **children's access assessment** to determine access to the service by minors (any individual under the age of 18).<br>• Services need extra **systems and processes** in place to stop minors from coming across content harmful to minors (e.g., by using age verification or another means of age assurance). This includes conducting a **child safety risk assessment** based on 'primary priority content' (pornography, self-harm, suicide),'priority content' (abusive, bullying content) and non-designated content (presents a material risk of significant harm to an number of children in the UK'. The 'Children's Risk Assessment Guidance and Risk Profiles' published by Ofcom includes a risk table that is useful for services.<br>• Services need to have highly effective age assurance in place where the service is likely to be accessed by children and allows harmful content (classed as primary priority content). Ofcom also recommends age assurance measures to protect children from other harmful content and from harmful features or behaviours.<br>• There is a duty on pornography sites to prevent minors from access (even if the sites do not contain user-to-user content), for example, by using age verification and keeping a written record of the measures taken to comply. | **Not directly included.** | **Safeguards for the protection of minors are included.**<br>• Safeguards are introduced by way of IMDA codes. The Code of Practice for Online Safety (CPOS) and the Content Code for Social Media Services (CCSMS) came into effect in July 2023 as a consolidated CPOS.<br>• The CPOS introduces community standards for the following content categories: sexual, violent, self-harm, cyberbullying, endangering public health, and facilitating vice and organized crime.<br>• The CPOS protects minors by requiring online communication services to provide targeted measures when minors access the specified content categories. Depending on age and severity, social media services are to provide safety information, limit exposure, or restrict access altogether.<br>• The CPOS requires user reporting tools and increased accountability. The exclusion for private or domestic communications suggests social media services may not be required to actively scan encrypted content for infringements.<br>• The CPOS requires designated social media services to disable access to specified harmful content or disallow specified online accounts related to content including: suicide and self-harm, sexual harm, public health, public security, and racial or religious disharmony or intolerance.<br>• The CPOS has greater powers and allows intervention even if there is no infringement of the social media services' own policies for all users in general, not only minors.<br>The IMDA released an inaugural Online Safety Assessment Report on Designated Social Media Services (DSMSs ) (the "Report") in February 2025. The Report assessed the comprehensiveness and effectiveness of the online safety measures implemented by DSMSs set out in the CPOS. The areas for improvement identified by the Report include the effectiveness of safety measures for children and user reporting measures (see Online Safety (Relief and Accountability) Bill below). | **Obligations for the protection of minors are included.**<br>Obligations include, without limitation:<br>• implementing privacy settings for children's accounts;<br>• implementing tools to enforce age restrictions (including age verification). Note that we were also expecting a newly published content age classification regime to be published by the National Media Authority. It remains to be seen how these requirements and regimes will overlap and operate;<br>• implementing blocking and filtering tools;<br>• providing parental control tools, including features that allow setting daily usage limits for children on digital platforms;<br>• providing tools for reporting child pornography and / or harmful content;<br>• leveraging technical capabilities, including AI systems, for the proactive detection, removal, or reporting of harmful content;<br>• immediate reporting to the authorities of any child pornography or harmful content;<br>• following orders issued by the authorities to remove or report child pornography, or any content harmful to children; and<br>• providing the authorities with periodic statistics and reports on the measures taken and extent of compliance.<br>The UAE Telecommunications And Digital Government Regulatory Authority **(TDRA)** will also issue policies directed at ISPs with respect to ensuring digital safety online (including with respect to content filtering and securing parental consent).<br>Caregivers are subject to separate requirements to monitor the children under their care and use parental controls provided by Digital Platforms to ensure safe usage.<br>Many of the obligations applicable to Digital Platforms, Caregivers and ISPs are subject to further clarification under subsequent decisions and implementing regulations to the Child Digital Safety Law. The requirements applicable to Digital Platforms may vary in their applicability depending upon the classification of the Digital Platform. |

| | DIGITAL SERVICES ACT (EU) | ONLINE SAFETY ACT (UK) | DIGITAL MARKETS ACT (EU) | BROADCASTING ACT (SG) | Child Digital Safety Law (UAE) |
|---|---|---|---|---|---|
| **Online advertising and commercial communications** | **Included.**<br>• Advertising content can itself constitute illegal content subject to the other rules applicable to that.<br>• Online platforms have to adopt measures for transparent online advertising to users and to show certain information, such as who is paying for and sponsoring the displayed ads, the target audience of the advertisements, and how and why it targets a user.<br>• Online platforms and VLOPs are limited on the use of sensitive, personal data for targeted advertising (e.g., to users with special characteristics such as ethnicity, political views, and sexual orientation).<br>• VLOPs are also required to keep databases of ads containing historic information as to the content and targeting of advertisements and the total number of recipients reached. This must be kept for one year after the advertisement was displayed for the last time. There is an extended list of transparency requirements (e.g., to contain the name of the product, service, or brand and information about any parameters used to exclude particular groups from receiving an ad), and the databases must also be accessible to vetted researchers on request and as appropriate and necessary to monitor or access compliance. | **Included.**<br>"Paid-for advertising may fall within 'user-generated content' where it is generated/uploaded/shared by a user and may be encountered by other users; however, the application of OSA safety duties to paid-for ads can be complex, and specific obligations also arise via the fraudulent advertising duties for categorised services." Not all paid-for advertisements are caught but may amount to a fraud offence. In this case, it is instead subject to the new **fraudulent advertising safety duties**.<br>• Category 1 service providers must use proportionate systems and processes designed to:<br>• (i) prevent individuals from encountering content consisting of fraudulent advertisements; (ii) minimize the length of time for which any such content is present; and (iii) swiftly take down such content when alerted to its presence or otherwise becoming aware of it.<br>• Category 2A services must operate the services using proportionate systems and processes designed to: (i) prevent individuals from encountering content consisting of fraudulent advertisements in or via search results of the service; (ii) minimize the length of time for which any such content is encountered in or via search results of the service; and (iii) once alerted, swiftly ensure that individuals are no longer able to encounter such content. Note: for search services, search content excludes paid-for advertisements.<br>• Category 1 and 2A services must include clear and accessible provisions in the terms of service and must provide information about any proactive technology used to comply with the above duties (including the kind of technology, when it is used, and how it works). Specific steps to address fraudulent advertising will be set out in Ofcom's codes of practice. | **Included.**<br>Gatekeepers are required to:<br>• Get **explicit consent** from consumers to **combine personal data** from other or third-party services with theirs for targeted advertising.<br>• Provide advertisers with **information** (e.g.,price- setting conditions and algorithms used by gatekeepers) so that they can conduct their own **independent review** of their advertising on the gatekeeper's platform.<br>• Allow their commercial users to **advertise their offer** and **freely conclude contracts** with their customers **outside the platform** (free choice of browser, virtual assistants, or search engines).<br>• Gatekeepers are prohibited from:<br>• Collecting end-user **personal data** across multiple platform services **without explicit consent** (in line with GDPR).<br>• Exploiting their **platform data** to compete with commercial users' services **without explicit consent**. | **Included separately.**<br>**Under the Advertising Standards Authority of Singapore (ASAS), the Singapore Code of Advertising Practice (SCAP), and the Guidelines for Interactive Marketing Communication & Social Media.**<br>• The SCAP requires all advertisements to be legal, decent, honest, and truthful.<br>• Specifically, online advertisements must be distinguished from personal/editorial content.<br>• Endorsements and commercial relationships must be fully disclosed.<br>• Dark patterns should not be used to conceal price, conditions, etc.<br>• Advertisements should be responsible and not subvert various shared or family values.<br>• Advertisements should conform to fair competition principles.<br>• For minors, the ASAS will consider their age, experience, and context of the advertising when assessing advertisements. Minors' personal information must not be disclosed unless authorized by law.<br>• Advertisements are assessed according to the advertisement's probable impact taken as a whole or in context.<br>• Advertisements that appear in Singapore are covered, regardless of origin. | **Child specific restrictions included.**<br>Digital Platforms are required to " activate....controls over targeted electronic advertisements, and tools to disable features related to excessive interaction and engagement by the child, in accordance with the age group".<br>Digital Platforms are prohibited from collecting, processing, publishing, or sharing personal data of children under the age of (13) thirteen for commercial purposes (including for the purpose of delivering targeted electronic advertisements).<br>There are also:<br>• strict advertising content requirements set out under the Federal Media Law and its implementing regulations (along with various sector specific advertising laws and regulations);<br>• direct marketing restrictions under various laws and regulations, including those issued by the TDRA; and<br>• restrictions on the use of personal data which would extend to online advertising related usage under Federal Personal Data Protection Law. |

| | DIGITAL SERVICES ACT (EU) | ONLINE SAFETY ACT (UK) | DIGITAL MARKETS ACT (EU) | BROADCASTING ACT (SG) | Child Digital Safety Law (UAE) |
|---|---|---|---|---|---|
| **Obligations – what do you have to do to comply?** | | | | | |
| **Summary** | **Obligations vary depending on the subcategory of service caught but center around four main principles: (i) transparency, (ii) empowering users, (iii) risk management obligations, and (iv) industry cooperation.** | **Overriding duty of care on all services in relation to illegal content, risk assessments, content reporting and complaints procedures, freedom of expression and privacy, and record keeping and review of records. Additional duties also apply to services likely to be accessible by minors and Category 1 services.** | **Obligations to regulate the anti-competitive behavior of a large digital group, which, as online platforms, hold a special and stable market position in the digital economy ("gatekeepers").** | **Overall duty to comply with codes of practice and directions from the IMDA to take steps the IMDA considers appropriate against egregious content.** | **Various obligations applicable to Digital Platforms, ISPs and Caregivers focused on minimising the exposure of children to harmful content online.** |
| **User controls, complaints and redress** | **Obligations for all platforms are included.**<br>• Existing obligation on all intermediary services to act expeditiously to remove illegal content once made aware of it to avoid liability.<br>• Terms must include details of policies and mechanisms for moderation.<br>• More detailed obligations on hosting services to have in place mechanisms to allow users to notify them of illegal content and to provide a statement of reasons to affected recipients in relation to actions taken.<br>• Online platforms must also have an internal complaint-handling system and allow for out-of-court dispute settlement.<br>• Online platforms must expedite complaints that come from "trusted flaggers."<br>• All online platforms that provide hosting services are required to put in place a notice mechanism for users to report illegal goods, services, or content online. | **Obligations for all platforms are included.**<br>• All services must have systems and processes in place that allow users to easily report illegal content or content harmful to minors.<br>• All services are also required to have a complaints procedure (which now also includes being able to make complaints about the use of proactive technology on the service resulting in content being taken down, given lower priority, or otherwise restricted and, for child-accessible services, a user being unable to access content because age verification/assurance measures have resulted in an incorrect assessment of the user's age).<br>• Provisions must be included in the terms of service setting out the processes that govern the handling and resolution of complaints.<br>• All services must include clear and accessible provisions in the terms of service informing users about their right to bring a claim for a breach of contract if their content is wrongly removed or if they are unjustifiably banned. | **Not included.**<br>• No user controls or redress but merger control of gatekeepers (see below). | **Obligations for all online communication services are included.**<br>• All online communication services are required to put in place user reporting mechanisms for harmful content such as those covered in the CPOS, and a resolution process for these reports.<br>• For accountability, designated online communication services must submit annual public accountability reports on the effectiveness of their measures against harmful content and their handling of user reports. The IMDA has not released exact reporting formats and requirements, but example reports submitted by the DSMS are available on the IMDA website.<br>• The Online Safety (Relief and Accountability) Bill is expected to come into force in 2026 and establish the Online Safety Commission (OSC). The OSC will initially focus on the five most prevalent and severe online harms: online harassment (including sexual harassment), intimate image abuse, image-based child abuse, doxxing, and online stalking. Victims, including minors, may submit reports of violations to the OSC and the OSC will be empowered to issue directions to the applicable service providers to address the violations. | **Obligations for Digital Platforms and ISPs.**<br>Digital Platform operators must provide clear and user-friendly tools for the immediate reporting of child pornography, harmful content, or harmful behaviours affecting children, and leverage their technical capabilities, including AI systems and machine learning algorithms, for the proactive detection, removal, or reporting of harmful content.<br>To process the personal data of children under the age of 13, Digital Platform operators must also (non-exhaustively): (i) obtain parental consent from the child's caregiver, ensuring that such consent is explicit, documented, and verifiable; (ii) provide a quick and easily accessible mechanism at all times to withdraw parental consent without complexity or negative consequences for the child; and (iii) clearly and understandably disclose the data privacy policy and the purpose of data collection to the child and their Caregiver.<br>ISPs must provide guidance tools and software that enable parental control and allow monitoring and supervision of the digital content accessed by children. |

| | DIGITAL SERVICES ACT (EU) | ONLINE SAFETY ACT (UK) | DIGITAL MARKETS ACT (EU) | BROADCASTING ACT (SG) | Child Digital Safety Law (UAE) |
|---|---|---|---|---|---|
| **Safety and risk management requirements** | **Safety and risk management obligations include:**<br>• VLOPs and VLOSEs are required to: (i) produce an annual risk assessment and independent audit; (ii) have risk mitigation/ reduction measures in place to prevent the misuse of their systems; and (iii) appoint a compliance officer.<br>• Providers of VLOPs should consider mitigating measures, such as moderation processes and ensuring the expeditious removal of any content constituting cyber violence.<br>• Online platforms with hosting services are required to report criminal offenses.<br>• Mechanisms for VLOPs and VLOSEs to adapt swiftly and efficiently in reaction to crises affecting public security or public health. This crisis response mechanism has been added in light of the Russian aggression in Ukraine and the particular impact on the manipulation of online information. It will be activated by the Commission on the recommendation of the board of national Digital Services Coordinators. It will make it possible to analyze the impact of the activities of VLOPs and VLOSEs on the crisis in question and decide on proportionate and effective measures to be put in place for the respect of fundamental rights.<br>• See also provisions regarding minors above. | **Safety and risk management obligations include:**<br>• All services must take steps to mitigate and manage risks of harm caused by illegal content (as identified by the risk assessment).<br>• All services are required to put in place appropriate systems and processes to improve user safety (e.g., to prevent individuals from encountering priority illegal content, minimize the duration of such content, and swiftly remove any illegal content).<br>• All services must carry out and maintain illegal content risk assessments (with each kind of content separately assessed). Content that is harmful to adults (but not designated by regulation) does not need to be addressed in the risk assessment.<br>• The systems and processes above apply across all areas of a service and, if proportionate, can include design of functionalities, algorithms and other features.<br>• Ofcom may (in limited circumstances) use Technology Notices to require use/ development of accredited technology in relation to CSEA and/or terrorism content.<br>• Set clear and accessible terms of service that state how users (including minors) are protected from illegal content, and enforce these terms consistently. The terms of service should separately address terrorism, child sexual exploitation and abuse (CSEA) and other priority illegal content, and should also specify what proactive technology is in place.<br>• All UK service providers must have systems and processes in place to assure (as far as possible) that detected and unreported CSEA content is reported to the National Crime Agency. A non-UK provider must report "UK-linked" CSEA content that is present on the service. This reporting requirement is not yet in force.<br>• See also provisions regarding minors above. | **Safety and risk management obligations include:**<br>• DMA imposes "self-executing" obligations and obligations that are "susceptible to specification." The latter means that gatekeepers must independently develop a concept for the adequate implementation of the conduct obligations. | **Currently, there are no safety and risk management requirements.** | **Various safety and risk managaement requirements.**<br>See "Protection of Minors" row, above. |

| | DIGITAL SERVICES ACT (EU) | ONLINE SAFETY ACT (UK) | DIGITAL MARKETS ACT (EU) | BROADCASTING ACT (SG) | Child Digital Safety Law (UAE) |
|---|---|---|---|---|---|
| **Record keeping and review** | **Record-keeping requirements include:**<br>• VLOPs and VLOSEs are required to have external and independent auditing of their risk management, including for their algorithmic systems.<br>• Online platforms need to keep records of moderation decisions to facilitate internal complaints and out of court settlement disputes.<br>• Providers need to keep various records to facilitate the transparency obligations set out below. | **Record-keeping requirements include:**<br>• All services must keep written records of all risk assessments (in an easily understandable form), including details about how the assessment was carried out and its findings, and records of any measure taken or in use to comply with its duties (including those recommended in Ofcom's codes of practice, as well as any alternative measures that are not recommended in the codes of practice and how these demonstrate compliance). Ofcom may require providers to provide information or documents relating to risk assessments (including the risk assessment record) where needed, and certain additional duties apply to categorised services.<br>• The OSA extends the list of requirements that can be subject to a skilled person's report (i.e., where providers are required to pay for and assist a skilled person to prepare a report about its compliance, if considered necessary by Ofcom). This includes requirements relating to minors' access assessments, user empowerment, fraudulent advertising, user identity verification, and CSEA content reporting. | **Currently, there are no specific record- keeping and review requirements.**<br>• Currently, there is no obligation to keep records, but the monitoring actions that the Commission may take include the imposition of an obligation on the gatekeeper to retain all documents deemed to be relevant to assess the gatekeepers' implementation of and compliance with these obligations and decisions.<br>• The status of all gatekeepers will be reviewed every four years, and any decision on changes will be adopted under the advisory procedure. | **Currently, there are no specific record-keeping and review requirements other than the user reporting and accountability measures described above in the "User controls and redress" section.** | **No specific record keeping requirements although ongoing monitoring and recording would be required to meet the reporting obligations set out in the row immediately below.** |
| **Transparency reporting obligations** | **Reporting obligations include:**<br>• All providers of intermediary services have to publish annual reports on content moderation, including the number of complaints received through the internal complaint-handling system, information on the use of automated tools, and the measures taken to provide training and assistance to persons in charge of content moderation.<br>• Online platforms and VLOPs have to publish transparency reports at least every six months on a variety of issues, including information such as the number of accounts that were suspended, content that was removed, and the time it took. VLOPs are also required to give access to the algorithms used for recommending content or products upon request of the EU Commission and member states, and within a reasonable time if necessary to monitor and assess compliance with the DSA. | **Reporting obligations include:**<br>• Transparency reporting duties apply to providers of certain regulated services (categorised services), who must publish transparency reports in accordance with Ofcom transparency notices. Services must publish the report in the specified format, submission and publication by the notice. Ofcom published final transparency reporting guidance in July 2025 and plans to issue draft/final transparency notices to categorised services in Summer 2026.<br>• Category 1 services are under a new duty to summarize in the terms of service the findings of the most recent illegal content risk assessment and minors' risk assessment. This includes information as to levels of risk, and as to nature and severity of potential harm. | **Reporting obligations include:**<br>• Gatekeepers are required to inform the Commission of a proposed c oncentration involving other platform providers from the digital sector. This obligation exists regardless of whether the merger would be subject to notification to the Commission or to a national antitrust authority under the relevant merger control rules.<br>• This mechanism will enable the Commission to monitor market developments in the digital sector and to become aware of "killer acquisitions" at an early stage.<br>• All gatekeepers are required to provide the Commission with an annual report describing in a detailed and transparent manner the measures it has implemented to ensure compliance with the obligations. A nonconfidential summary also needs to be published annually. | **Currently, there are no specific transparency reporting requirements other than the user reporting and accountability measures described above in the "User controls and redress" section.** | **Digital Platform operators are required to provide periodic statistics and reports on the measures they have taken to comply with the Child Digital Safety Law (as well as the extent of their compliance).**<br>In addition there are various reporting obligations with respect to any identified Child Pornography applicable to each of ISPs, Digital Platforms and Caregivers.<br>Digital Platform operators are also required to provide periodic disclosure of their policies regarding dealing with users and content.<br>Digital Platform operators are also required to clearly and understandably disclose the data privacy policy and the purpose of data collection to the child and their Caregiver, where processing the personal data of under 13s. |

| | DIGITAL SERVICES ACT (EU) | ONLINE SAFETY ACT (UK) | DIGITAL MARKETS ACT (EU) | BROADCASTING ACT (SG) | Child Digital Safety Law (UAE) |
|---|---|---|---|---|---|
| **Other obligations** | **In addition to the above, there are other obligations that also apply:**<br>• All service providers without an establishment in the EU must appoint a **legal representative** in a member state where they offer services.<br>• VLOPs and VLOSEs have to offer users a system for recommending content that is not based on profiling (so that users can enforce their right to opt out from content recommendations based on profiling).<br>• Online platforms that are marketplaces must establish know-your-customer-type protocols for merchants using their platforms and adopt new technologies to verify and check traceability information provided by traders that sell via platforms to consumers. This obligation on traceability of business users in online marketplaces will help identify sellers of illegal goods or reasonable efforts by online marketplaces to randomly check whether products or services have been identified as being illegal in any official database.<br>• Online platforms that are marketplaces are also required to display **trader information** to users and to vet the credentials of any third-party suppliers. This especially includes provision of access to vetted researchers to the key data of the largest platforms and provision of access to NGOs regarding access to public data, to provide more insight into how online risks evolve.<br>• All service providers must include clear information on any **content restrictions in their terms of service**. Platforms must clearly describe their recommendation systems in their terms and conditions. Platforms also must allow users to modify the parameters used in the recommendation systems and must include at least one option not based on profiling (as already described in the "Online advertising" section, above). | **In addition to the above, there are other obligations that also apply:**<br>• Category 1 services are under a duty to **empower adult users**. This includes making features available to all adult users that result in the use of systems and processes designed to reduce the likelihood of the user encountering or to alert them to harmful content.<br>• Category 1 services are under a duty to offer adult users the option to **verify their identity** where such verification is not required for access to the service. The verification process may be of any kind (and does not require the providing of documentation). | **In addition to the above, there are other obligations that also apply:**<br>• Positive obligation on gatekeepers to ensure that users have the right to unsubscribe from core platform services, ensure interoperability (including of instant messaging services), and provide access to marketing and advertising data.<br>• Obligation on gatekeepers not to engage in self-preferencing, reuse certain private data, establish unfair conditions for business users, pre-install certain software, or require app developers to use certain services.<br>• Large messaging services have to open up and **interoperate** with smaller messaging platforms (i.e., allow the exchange of messages, files, and calls across messaging apps). Interoperability obligations/ provisions for social networks will be assessed in the future.<br>• Gatekeepers are required to offer **fair and nondiscriminatory terms and conditions** when using online sales platforms for application software. They need to ensure that commercial users are **free to use, offer, or cooperate with their identification services**. This includes the right of end users to unsubscribe from core platform services such that the conditions of termination can be exercised without undue difficulty.<br>• Gatekeepers are prohibited from engaging in unfair conditions for business users such as **bundling** (i.e., making the use of a core platform service dependent on the use of another core platform service) and **preventing** commercial users from offering their products and services on third-party platforms at **different terms and prices**. This also includes restricting gatekeepers from **forcibly registering end users** with other proprietary platform services without explicit consent. | **In addition to the above, there are other obligations that also apply:**<br>• Online communication services have a duty to take all practicable steps to comply with codes of practice issued by the IMDA as well as guidelines from the ASAS and the Personal Data Protection Commission (PDPC).<br>• Online communication services must take actions including disabling access to egregious content by Singapore end users, stopping delivery or communication to accounts of Singapore end users or groups of end users including Singapore end users. This includes blocking the content or blocking the account that communicates the content.<br>• In noncompliance or extreme cases, access to that online communication service via Internet access services is blocked entirely. | The key obligations applicable to ISPs and Digital Platforms have been summariesd in the rows above.<br><br>Note that the Child Digital Safety Law is not the only law regulating online content and digital platforms in the UAE and that additional obligations are set out under:<br>• the Federal Media Law and its implementing regulations<br>• the TDRA Internet Guidelines;<br>• the Personal Data Protection Law;<br>• the Trading by Modern Technological Means Law;<br>• Wadeema's Law; and<br>• the Cybercrime Law. |

| | DIGITAL SERVICES ACT (EU) | ONLINE SAFETY ACT (UK) | DIGITAL MARKETS ACT (EU) | BROADCASTING ACT (SG) | Child Digital Safety Law (UAE) |
|---|---|---|---|---|---|
| **Sanctions and enforcement** | | | | | |
| **Regulator** | **Each member state must designate a "digital services coordinator" (DSC), which will be supported by the European Board for Digital Services.**<br>• DSCs will be responsible for ensuring compliance with the DSA, verifying platform user numbers in the EU, and designating platforms as VLOPs at least every six months.<br>• Powers include carrying out on-site inspections, interviewing staff members, and requiring the production of documents and information.<br>**Commission**<br>• The Commission will produce codes of conduct to facilitate compliance with the DSA, including on topics such as child protection or accessibility, disinformation, and online hate. Compliance with these codes also becomes binding with regard to the DSA.<br>• The Commission has been conferred exclusive and enhanced supervision and enforcement powers to supervise VLOPs and VLOSEs for the obligations specific to this type of actor. They will be supervised at European level in cooperation with the member states.<br>• VLOPs must pay the European Commission a supervisory fee of up to 0.05% of their global annual revenue to enforce the DSA. | **Ofcom**<br>• Ofcom is required to: (i) publish codes of practice (e.g., on terrorism and child exploitation content, and certain recommendations on the use of proactive technology), (ii) establish an appeals and super-complaints function, and (iii) establish appropriate mechanisms for user advocacy.<br>• Providers can follow Ofcom's Codes of Practice or take alternative effective measures to meet the legal duties.<br>• Ofcom will produce further guidance to assist in complying with record keeping and review duties and minors' access assessment duties in consultation with the ICO.<br>• Ofcom is also permitted to carry out inspections and audits. | **Commission**<br>• The Commission is a sole enforcer, but it can engage in regulatory dialogue.<br>• An advisory committee and a high-level group will be set up.<br>• Monitoring, investigation, and enforcement powers include power to request information, conduct dawn raids, impose interim measures, and accept commitments. It also includes the ability to specify concrete measures to be implemented by the gatekeeper concerned if the measures it has taken to date do not ensure effective compliance with the DMA requirements.<br>**Member states**<br>• Member states can empower national competition authorities to start investigations and transmit their findings to the Commission. | **Infocomm Media Development Authority**<br>• The IMDA is responsible for issuing orders to block or take down egregious content.<br>• The IMDA provides practical guidance for online communications services via codes of practice.<br>**Personal Data Protection Commission**<br>• The PDPC is responsible for ensuring that the personal data of individuals is not misused.<br>• The PDPC provides practical guidance via Advisory Guidelines, in addition to the Personal Data Protection Act 2012 and the Personal Data Protection Regulations 2021.<br>**Advertising Standards Authority of Singapore**<br>• The ASAS is responsible for developing a code of advertising practices for advertisements and investigating breaches.<br>• The ASAS provides practical guidance via guidelines for specific types of advertisements. | **The newly established Child Digital Safety Council to be chaired by the Minister of Family is the primary authority resposible for the implementation of the Child Digital Safety Law.**<br>Various other regulators have duties and powers in connection with digital content and data regulation outside the scope of the Child Digital Safety Law (or alongside it), including:<br>• TDRA;<br>• National Media Authority; and<br>• UAE Data Office. |

| | DIGITAL SERVICES ACT (EU) | ONLINE SAFETY ACT (UK) | DIGITAL MARKETS ACT (EU) | BROADCASTING ACT (SG) | Child Digital Safety Law (UAE) |
|---|---|---|---|---|---|
| **How will companies be sanctioned?** | **Notable punishments include:**<br>• Fines – Up to 6% of global annual turnover. Member states or the Commission may also impose fines of up to 1% of annual income or turnover of the provider or platform for providing incorrect, incomplete, or misleading information in response to a request for information.<br>• Interference – DSCs can impose interim measures and order the cessation of infringements.<br>• Individuals – Instead of going through the complaint-handling system or out-of-court procedure (as mentioned in the "User controls, complaints and redress" section), individuals can initiate legal proceedings against the platforms. | **Notable punishments include:**<br>• Fines – Up to 10% of global turnover or £18 million (whichever is higher).<br>• Interference – Ofcom can apply to the court for business disruption measures in the most serious cases of non-compliance. These include service restriction orders to restrict access to platforms or access restriction orders to block access.<br>• Criminal sanctions – Against named senior managers of offending companies. The OSA has extended the list of offenses for which a named director can be held liable. The defenses available vary depending on the offense committed. Criminal offences exist in specific circumstances, particularly around compliance with Ofcom's enforcement/ information-gathering powers. These offences came into force in from 10 January 2024. | **Notable punishments include:**<br>• Fines – up to 10% of a gatekeeper's total worldwide turnover (20% for a repeat offense).<br>• Market investigation – by the Commission, which could potentially lead to behavioral or structural remedies if a gatekeeper systematically fails to comply with the DMA (at least three breaches in eight years). | **Notable punishments include:**<br>• Fines – The IMDA imposes fines up to SG $1 million and a further fine not exceeding SG $100,000 for every day or part thereof the offense continues after conviction. The PDPC imposes fines up to SG $1 million or up to 10% of annual Singapore turnover (whichever is higher).<br>• Directions – by the IMDA, including written directions to disable access to egregious content or access to the account posting egregious content, as well as blocking directions to block entire online communications services. The PDPC can also issue directions to organizations to take remedial steps, as well as accept voluntary undertakings. When the OSC is established, it will have powers to issue directions to platforms, administrators of groups or pages, content communicators, internet service providers or app stores to take down harmful content, suspend offending accounts, disable access and allow the victim to post a reply.<br>• The ASAS Code and Guidelines do not impose fines/ directions and are based on self-regulation. | **Penalties are to be set out under a separate Administrative Penalties Regulation.**<br><br>Digital Platforms can already be blocked (in whole or in part) by the TDRA, with the support of local telecommunications providers (or, with the support of local app store providers where those do not comply with the TDRA Internet Guidelines (see here). This power is expressly reflected in the Child Digital Safety Law. The Internet Guidelines apply regardless of the territory from which the relevant website, platforms and / or mobile application is made available. |

| | DIGITAL SERVICES ACT (EU) | ONLINE SAFETY ACT (UK) | DIGITAL MARKETS ACT (EU) | BROADCASTING ACT (SG) | Child Digital Safety Law (UAE) |
|---|---|---|---|---|---|
| | | | **Exemptions** | | |
| **Exemptions** | **Freedom of speech.**<br>• Services must mitigate how their content moderation systems impact freedom of expression. | **Freedom of speech, privacy, and journalistic exemption.**<br>• All services have a duty to protect users' rights to freedom of expression and privacy within the law. In addition, a Category 1 service provider must specify in a publicly available statement the "positive steps" it has taken to protect against these rights.<br>• (Once commenced) services will have duties about acting against users consistently with their terms of service.<br>• Category 1 service providers are also required to balance their obligations in relation to harmful content, with a separate obligation to protect information of democratic importance and journalistic content. It is up to the provider to determine what it "reasonably considers" to be journalistic content or content of democratic importance for purposes of applying the terms of service.<br>• News publisher content is excluded from "regulated user-generated content" (so it is not subject to platforms' core safety duties), and once commence Category 1 services will have specific duties to protect news publisher and journalistic content (including tailored notice/appeals mechanisms).<br>• Individuals have the right to appeal content removal and platforms need to put in place fast-tracked appeals processes for producers of journalistic content. | **Public interest reasons.**<br>• On limited grounds of public health or public security, the Commission will have discretion on whether the obligation applies to specific core platform services.<br>• The Commission will need to review the exemption decision at least every year and decide whether to either wholly or partially lift the exemption.<br>• Gatekeepers will not be able to rely on the grounds of exemption based on public morality. | **Private or domestic nature.**<br>• Directions and orders to restrict egregious content do not apply to communications of a private or domestic nature. | **None** |

| | DIGITAL SERVICES ACT (EU) | ONLINE SAFETY ACT (UK) | DIGITAL MARKETS ACT (EU) | BROADCASTING ACT (SG) | Child Digital Safety Law (UAE) |
|---|---|---|---|---|---|
| **Timeline** | | | | | |
| **Exemptions** | **Formally adopted.**<br>• The Digital Services Act entered into force on November 16, 2022.<br>• The European Commission designated 19 VLOPS and 2 VLOSEs on April 25, 2023. These platforms had four months, until August 25, 2023, to become fully compliant with the DSA.<br>• All other intermediary services will have to ensure compliance by February 17, 2024. | **Formally adopted.**<br>The Online Safety Bill received Royal Assent and became an Act in UK law on October 26, 2023.<br>• After providing companies with a transition period to prepare for its enforcement, as of:<br>• 17 March 2025 - platforms have a legal duty to protect their users from illegal content online.<br>• 25 July 2025 – platforms have a legal duty to protect children online.<br>• 10 February 2026 – Ofcom publishes final guidance on the Online Safety Act super complaints regime<br>• April 2026 – Ofcom plans to issue final Technology Notices guidance<br>• July 2026 – Ofcom plans to issue register of categorised services. Ofcom expects to issue transparency notices to categorised services within a few weeks of this date.<br>• July 2026 – Ofcom plans to issue statutory report on age assurance.<br>• Autumn 2026 – Ofcom plans to publish its "Additional Safety Measures" statement (additional measures relating to the illegal content and children's Codes of Practice).<br>• October 2026 – Ofcom plans to issue statutory report on content harmful to children.<br>• 1 November 2026 – Ofcom plans to issue Online Information Advisory Committee statutory report.<br>• January 2027 – Ofcom plans to publish statutory report on app stores. | **Formally adopted.**<br>• The DMA entered into force on November 1, 2022. However, most provisions of the Act became applicable in May 2023.<br>• The gatekeepers were officially appointed on September 6, 2023 and they are required to comply with their obligations by March 6, 2024, six months following designation. | **Formally adopted.**<br>• The Online Safety (Miscellaneous Amendments) Bill had its first reading on October 3, 2022. The second reading occurred in November 2022. Subsequently, the Bill was passed and came into force in February 2023.<br>• The Code of Practice for Online Safety and Content Code for Social Media Services were released in draft form for public consultation from July to August 2022. The final fused code, Code of Practice for Online Safety, came into force in July 2023.<br>• The PDPC and ASAS legislation/guidelines are already in force.<br>• Further guidelines will be updated from time to time by the IMDA, PDPC, and ASAS, respectively. The PDPC released Advisory Guidelines on the PDPA for Children's Personal Data in the Digital Environment in March 2024.<br>To be **formally adopted.**<br>• The Online Safety (Relief and Accountability) Bill (OSRA) had its first reading on October 15, 2025. The second reading occurred on November 5, 2025 and the OSRA was passed on the same day.<br>• It has not come in force but is expected to do so later in 2026. | **Formally adopted.**<br>• The Child Digital Safety Law came into force on 1 January 2026.<br>• We are awaiting a decision on the classification of Digital Platforms and the Administrative Penalties Resolution (along with, potentially, additional implementing decisions and / or guidance documents). |