






Online Harms: a comparison of the UK, EU and Singapore legislation


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) and the consultation and proposed updates to the Singapore Broadcasting Act as of November 2023.

	DIGITAL SERVICES ACT (EU)	ONLINE SAFETY BILL (UK)	DIGITAL MARKETS ACT (EU)	BROADCASTING ACT (SG)
	Scope			
<p>Whom it applies to</p> 	<p>“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:</p> <ul style="list-style-type: none"> • Hosting services: platforms which store information -provided by the recipient of the service. • 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. • Very large online platforms (VLOPs): platforms with more than 10% of the 450 million monthly active users in the EU. • Very large search engines (VLOSEs) with more than 10% of the 450 million consumers in EU. <p>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.</p>	<p>Services that provide online user interactions and user-generated content and search services</p> <ul style="list-style-type: none"> • Services covered include social media platforms, consumer cloud storage sites, video-sharing platforms, online forums, gaming sites, online marketplaces, and search engines. • 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.” • There are certain separate duties that apply specifically to internet services that display or publish pornographic content. <p>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.</p>	<p>Platforms acting as digital “gatekeepers” to the single market</p> <p>A platform qualifies as a gatekeeper if it operates a “core platform service” whereby:</p> <ul style="list-style-type: none"> • 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; • It has at least 45 million monthly end users and at least 10,000 business users in the EU. <p>“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.</p> <p>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.</p> <p>The European Commission announced companies it considers to be gatekeepers here on September 6, 2023.</p>	<p>Online communication services that have “significant reach or impact”</p> <p>An online communication service is covered if it has significant reach or impact. This includes electronic services with the following characteristics:</p> <ol style="list-style-type: none"> 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); b. The service allows end users to communicate content on the service; and c. Any other characteristics prescribed by Infocomm Media Development Authority (IMDA) regulations. <p>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.</p>

	DIGITAL SERVICES ACT (EU)	ONLINE SAFETY BILL (UK)	DIGITAL MARKETS ACT (EU)	BROADCASTING ACT (SG)
Scope				
Territorial scope 	Online intermediary services offering their services in the EU.	Service with links to the UK A service has links to the UK if: <ul style="list-style-type: none"> • It has a significant number of UK users; or • UK users form one or the only target market for the service; or • 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. A service has links to Singapore if: <ul style="list-style-type: none"> • The service is between a point in Singapore and one or more other points in Singapore; or • The service is between a point outside Singapore and at least one point in Singapore.
What type of content is covered? 	Illegal content. <ul style="list-style-type: none"> • 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 legal but harmful content. <ul style="list-style-type: none"> • 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. • 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. • 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). • Provisions relating to content that is harmful to adults were removed from the final text. 	Not directly covered.	“Egregious” content, including content that may otherwise be legal. <ul style="list-style-type: none"> • Egregious content means content that advocates or instructs on: <ul style="list-style-type: none"> • Suicide or self-harm; • Violence or cruelty or other infliction of serious physical harm on human beings; • Sexual violence, depicting child nudity for a sexual purpose, or exploiting child nudity in an offensive way; • Conduct that is likely to obstruct public health measures or result in a public health risk in Singapore; • 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 • Terrorism and any other content prescribed by IMDA regulations. • Whether the content is conducted within or outside Singapore is immaterial. <p>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.</p>

	DIGITAL SERVICES ACT (EU)	ONLINE SAFETY BILL (UK)	DIGITAL MARKETS ACT (EU)	BROADCASTING ACT (SG)
	Scope			
<p>Protection of minors</p> 	<p>Obligations for the protection of minors are included.</p> <ul style="list-style-type: none"> • Online platforms are required to have appropriate and proportionate measures to ensure a high level of privacy, safety, and security for minors. • VLOPs need to have reasonable, proportionate, and effective mitigation measures (tailored to risks), which may include age verification. • Bans on targeted advertisements to minors based on profiling of their personal data. • 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. • Additional obligations on VLOPs and VLOSEs to protect minors, including assessments. • Note: “minors” means an individual under the age of 18. 	<p>Specific duties if services are likely to be accessed by minors.</p> <ul style="list-style-type: none"> • Services have to carry out a child accessibility assessment to determine: (i) whether it is possible for minors in the UK to access the service (or any part of it); (ii) whether there are a significant number of child users of the service; or (iii) whether the service is of a kind likely to attract a significant number of child users (not further defined). • 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 (which requires separate consideration of minors in different age groups and minors who have certain characteristics or are members of a certain group, the specifics of which still remain unclear), implementing mitigations to protect minors, and making certain information available in the terms of service (e.g., how minors are prevented from encountering illegal/harmful content and how they are determined to be at risk of harm). • There is also 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. • Note “minors” means an individual under the age of 18. 	<p>Not directly included.</p>	<p>Safeguards for the protection of minors are included.</p> <ul style="list-style-type: none"> • 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) were released for public consultation in 2022 and came into effect in July 2023 as a fused CPOS. • The CPOS introduces community standards for the following content categories: sexual, violent, self-harm, cyberbullying, endangering public health, and facilitating vice and organized crime. • 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. • 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. • 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. <p>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.</p>

	DIGITAL SERVICES ACT (EU)	ONLINE SAFETY BILL (UK)	DIGITAL MARKETS ACT (EU)	BROADCASTING ACT (SG)
	Scope			
<p>Online advertising and commercial communications</p> 	<p>Included.</p> <ul style="list-style-type: none"> Advertising content can itself constitute illegal content subject to the other rules applicable to that. 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. 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). 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. 	<p>Included.</p> <p>A paid-for advertisement can now qualify as user-generated content and is therefore subject to the various safety duties that apply to such content (i.e., covering illegal content and content that is harmful to minors).</p> <p>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.</p> <ul style="list-style-type: none"> Category 1 service providers must use proportionate systems and processes designed to: (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. 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. 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. 	<p>Included.</p> <p>Gatekeepers are required to:</p> <ul style="list-style-type: none"> Get explicit consent from consumers to combine personal data from other or third-party services with theirs for targeted advertising. 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. 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). Gatekeepers are prohibited from: <ul style="list-style-type: none"> Collecting end-user personal data across multiple platform services without explicit consent (in line with GDPR). Exploiting their platform data to compete with commercial users' services without explicit consent. 	<p>Included separately.</p> <p>Under the Advertising Standards Authority of Singapore (ASAS), the Singapore Code of Advertising Practice (SCAP), and the Guidelines for Interactive Marketing Communication & Social Media.</p> <ul style="list-style-type: none"> The SCAP requires all advertisements to be legal, decent, honest, and truthful. Specifically, online advertisements must be distinguished from personal/editorial content. Endorsements and commercial relationships must be fully disclosed. Dark patterns should not be used to conceal price, conditions, etc. Advertisements should be responsible and not subvert various shared or family values. Advertisements should conform to fair competition principles. 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. Advertisements are assessed according to the advertisement's probable impact taken as a whole or in context. <p>Advertisements that appear in Singapore are covered, regardless of origin.</p>

	DIGITAL SERVICES ACT (EU)	ONLINE SAFETY BILL (UK)	DIGITAL MARKETS ACT (EU)	BROADCASTING ACT (SG)
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.
User controls, complaints and redress 	Obligations for all platforms are included. <ul style="list-style-type: none"> Existing obligation on all intermediary services to act expeditiously to remove illegal content once made aware of it to avoid liability. Terms must include details of policies and mechanisms for moderation. 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. Online platforms must also have an internal complaint-handling system and allow for out-of-court dispute settlement. Online platforms must expedite complaints that come from “trusted flaggers.” 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 services are included. <ul style="list-style-type: none"> All services must have systems and processes in place that allow users to easily report illegal content or content harmful to minors. 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). Provisions must be included in the terms of service setting out the processes that govern the handling and resolution of complaints. 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. <ul style="list-style-type: none"> No user controls or redress but merger control of gatekeepers (see below). 	Obligations for all online communication services are included. <ul style="list-style-type: none"> 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. 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.

DIGITAL SERVICES ACT (EU)

ONLINE SAFETY BILL (UK)

DIGITAL MARKETS ACT (EU)

BROADCASTING ACT (SG)

Obligations – what do you have to do to comply?

Safety and risk management requirements



Safety and risk management obligations include:

- 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**.
- Providers of VLOPs should consider mitigating measures, such as moderation processes and ensuring the expeditious removal of any content constituting cyber violence.
- Online platforms with hosting services are required to **report criminal offenses**.
- 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.
- See also provisions regarding minors above.



Safety and risk management obligations include:

- All services must take steps to mitigate and manage risks of harm caused by illegal content (as identified by the risk assessment).
- 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).
- 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.
- The systems and processes above apply across all areas of a service and, if proportionate, can include design of functionalities, algorithms and other features.
- Ofcom can require services to use proactive technology to comply with duties regarding illegal content, minors' online safety and fraudulent advertising.
- 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.
- 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.
- See also provisions regarding minors above.

Safety and risk management obligations include:

- 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.

	DIGITAL SERVICES ACT (EU)	ONLINE SAFETY BILL (UK)	DIGITAL MARKETS ACT (EU)	BROADCASTING ACT (SG)
Obligations – what do you have to do to comply?				
Record keeping and review 	<p>Record-keeping requirements include:</p> <ul style="list-style-type: none"> VLOPs and VLOSEs are required to have external and independent auditing of their risk management, including for their algorithmic systems. Online platforms need to keep records of moderation decisions to facilitate internal complaints and out of court settlement disputes. Providers need to keep various records to facilitate the transparency obligations set out below. 	<p>Record-keeping requirements include:</p> <ul style="list-style-type: none"> 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). Category 1 services must supply Ofcom with a full copy of the assessment records. The updated 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 now also includes requirements relating to minors’ access assessments, user empowerment, fraudulent advertising, user identity verification, and CSEA content reporting. 	<p>Currently, there are no specific record-keeping and review requirements.</p> <ul style="list-style-type: none"> 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. The status of all gatekeepers will be reviewed every four years, and any decision on changes will be adopted under the advisory procedure. 	<p>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.</p>
Transparency reporting obligations 	<p>Reporting obligations include:</p> <ul style="list-style-type: none"> 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. 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. 	<p>Reporting obligations include:</p> <ul style="list-style-type: none"> All services must publish annual transparency reports. Exactly what should be included and other details regarding format, submission, and publication are to be defined by Ofcom. 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. 	<p>Reporting obligations include:</p> <ul style="list-style-type: none"> Gatekeepers are required to inform the Commission of a proposed concentration 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. 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. 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. 	<p>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.</p>

DIGITAL SERVICES ACT (EU)

ONLINE SAFETY BILL (UK)

DIGITAL MARKETS ACT (EU)

BROADCASTING ACT (SG)

Obligations – what do you have to do to comply?

Other obligations



In addition to the above, there are other obligations that also apply:

- All service providers without an establishment in the EU must appoint a **legal representative** in a member state where they offer services.
- 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).
- 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.
- 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.
- 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:



- Category 1 services are under a new 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.
- Category 1 services are under a new 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:

- 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.
- 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.
- 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.
- 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.
- 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:

- 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).
- 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.
- In noncompliance or extreme cases, access to that online communication service via Internet access services is blocked entirely.

	DIGITAL SERVICES ACT (EU)	ONLINE SAFETY BILL (UK)	DIGITAL MARKETS ACT (EU)	BROADCASTING ACT (SG)
Sanctions and enforcement				
Regulator 	<p>Each member state must designate a “digital services coordinator” (DSC), which will be supported by the European Board for Digital Services.</p> <ul style="list-style-type: none"> 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. Powers include carrying out on-site inspections, interviewing staff members, and requiring the production of documents and information. <p>Commission</p> <ul style="list-style-type: none"> 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. 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. VLOPs must pay the European Commission a supervisory fee of up to 0.05% of their global annual revenue to enforce the DSA. 	<p>Ofcom</p> <ul style="list-style-type: none"> 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. Ofcom’s codes of practices will not be mandatory. 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. Ofcom is also permitted to carry out inspections and audits. 	<p>Commission</p> <ul style="list-style-type: none"> The Commission is a sole enforcer, but it can engage in regulatory dialogue. An advisory committee and a high-level group will be set up. 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. <p>Member states</p> <ul style="list-style-type: none"> Member states can empower national competition authorities to start investigations and transmit their findings to the Commission. 	<p>Infocomm Media Development Authority</p> <ul style="list-style-type: none"> The IMDA is responsible for issuing orders to block or take down egregious content. The IMDA provides practical guidance for online communications services via codes of practice. <p>Personal Data Protection Commission</p> <ul style="list-style-type: none"> The PDPC is responsible for ensuring that the personal data of individuals is not misused. The PDPC provides practical guidance via Advisory Guidelines, in addition to the Personal Data Protection Act 2012 and the Personal Data Protection Regulations 2021. <p>Advertising Standards Authority of Singapore</p> <ul style="list-style-type: none"> The ASAS is responsible for developing a code of advertising practices for advertisements and investigating breaches. <p>The ASAS provides practical guidance via guidelines for specific types of advertisements.</p>
How will companies be sanctioned? 	<p>Notable punishments include:</p> <ul style="list-style-type: none"> 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. Interference – DSCs can impose interim measures and order the cessation of infringements. 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. 	<p>Notable punishments include:</p> <ul style="list-style-type: none"> Fines – Up to 10% of global turnover or £18 million (whichever is higher). Interference – Requiring Internet service providers to block access to sites and third parties to withdraw access to key services. 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. Ofcom will begin enforcing against senior executives within two months (rather than two years) of the OSA coming into effect. 	<p>Notable punishments include:</p> <ul style="list-style-type: none"> Fines – up to 10% of a gatekeeper’s total worldwide turnover (20% for a repeat offense). 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). 	<p>Notable punishments include:</p> <ul style="list-style-type: none"> 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). 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. The ASAS Code and Guidelines do not impose fines/directions and are based on self-regulation.

	DIGITAL SERVICES ACT (EU)	ONLINE SAFETY BILL (UK)	DIGITAL MARKETS ACT (EU)	BROADCASTING ACT (SG)
Exemptions				
Exemptions 	Freedom of speech. <ul style="list-style-type: none"> Services must mitigate how their content moderation systems impact freedom of expression. 	Freedom of speech, privacy, and journalistic exemption. <ul style="list-style-type: none"> 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. All services have a duty not to take down or restrict content, ban, or suspend users, except as set out in the terms of service. 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. Recognized news publishers' content is not in scope of the OSA. Individuals have the right to appeal content removal. 	Public interest reasons. <ul style="list-style-type: none"> On limited grounds of public health or public security, the Commission will have discretion on whether the obligation applies to specific core platform services. The Commission will need to review the exemption decision at least every year and decide whether to either wholly or partially lift the exemption. Gatekeepers will not be able to rely on the grounds of exemption based on public morality. 	Private or domestic nature. <ul style="list-style-type: none"> Directions and orders to restrict egregious content do not apply to communications of a private or domestic nature.
Time line				
Time line 	Formally adopted. <ul style="list-style-type: none"> The Digital Services Act entered into force on November 16, 2022. 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. All other intermediary services will have to ensure compliance by February 17, 2024. 	Formally adopted. <p>The Online Safety Bill received Royal Assent and became an Act in UK law on October 26, 2023.</p> <ul style="list-style-type: none"> On October 26, 2023, Ofcom published its approach to implementing the OSA. Ofcom's timeline specifies that certain parts of the Act will not come into force until 2026. Risk assessments are expected to be completed by: <ul style="list-style-type: none"> Q4 of 2024 for the illegal harms risk assessment. Q2 of 2025 for the minors' access assessment. Q3 of 2025 for the minors' risk assessment. 	Formally adopted. <ul style="list-style-type: none"> The DMA entered into force on November 1, 2022. However, most provisions of the Act became applicable in May 2023. 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. <ul style="list-style-type: none"> 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. 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. The PDPC and ASAS legislation/guidelines are already in force. Further guidelines will be updated from time to time by the IMDA, PDPC, and ASAS, respectively. A further consultation was launched in August 2023 by the PDPC on advisory guidelines for the use of minors' data.