





Online Harms: A comparison of the UK/EU legislative proposals



Following on from our [previous overview](#) of the European Union Digital Services Act (“**DSA**”) and UK’s Online Safety Bill (“**OSB**”) back in January this year, this table sets out a high-level comparison of the updated proposals as at May 2022, alongside a further comparison of the European Union Digital Markets Act (“**DMA**”).

Bold text indicates new or amended material from the updated versions of the DSA and OSB since our last update.

b>

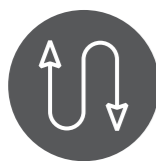
| | DIGITAL SERVICES ACT (EU) | ONLINE SAFETY BILL (UK) | DIGITAL MARKETS ACT (EU) |
|---|---|--|---|
| Scope | | | |
| Who it applies to  | <p>“Online intermediary services.” There are sub-categories of:</p> <ul style="list-style-type: none"> • Intermediary service: platforms offering network infrastructure, including Internet access providers and domain name registrars. • Hosting services: cloud computing and webhosting services. • Online platforms: platforms bringing together sellers and consumers, such as online marketplaces, app stores, collaborative economy platforms and social media platforms. • 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 will 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.” | <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 EUR 7.5 billion within the EU in the past three years, or has a market valuation of at least EUR 75 billion; and • It has at least 45 million monthly end users and at least 1 0,000 business users in the EU. <p>“Core platform services” include web browser and voice assistants among others, but excludes connected TVs.</p> <p>SMEs are exempt from being gatekeepers, apart from in exceptional cases. However, there is a category of “emerging gatekeeper” meaning that the Commission can impose obligations on companies whose competitive position is proven but not yet sustainable.</p> |
| Territorial scope  | <p>Online intermediary services offering their services in the EU.</p> | <p>Service with links to the UK.</p> <p>A service has links to the UK if:</p> <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). | <p>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.</p> |

| | | | |
|---|--|--|---|
| <p>What type of content/activity is covered?</p>  | <p>Unlawful content or content which may have negative effects for the exercise of fundamental rights or intentional manipulation of services with an action or foreseeable effect on public health, minors, civic disclosure, electrical process or public security.</p> <ul style="list-style-type: none"> • Unlawful content is content which is unlawful under national or EU laws, such as hate speech, terrorist propaganda and intellectual property infringement, or relates to activities that are illegal, such as the sharing of images depicting child sexual abuse. • As well as illegal content, the DSA also covers illegal goods and services. • It is unclear whether the DSA covers private communications. To the extent that private communication services also double as an intermediary service (or another category of provider), they may also become subject to the DSA, but the provisional agreement of the final text has not been published yet and the point remains unclear. | <p>Illegal content and legal but harmful content.</p> <ul style="list-style-type: none"> • Illegal content means content which (including the dissemination, possession or accessing of which) amounts to a relevant offence; the definition no longer refers to content which the provider of the services has reasonable grounds to believe amounts to a relevant offence. This covers terrorism offences, offences related to child sexual exploitation and abuse, and other priority categories including assisting suicide; threats to kill; public order offences, harassment, stalking; and fear or provocation of violence; supply of drugs and psychoactive substances; offences relating to firearms and other weapons; assisting illegal immigration; sexual exploitation; offences relating to sexual images; offences relating to proceeds of crime; fraud; offences relating to financial services, including misleading statements and impressions; and inchoate offences (e.g. attempting, conspiring to commit, encouraging, assisting, aiding, abetting, counselling or procuring to commit any of these offences). • Content is harmful to children/adults if either: (i) it is designated as such in regulations to be made by the Secretary of State, or (ii) it is content (outside of (i) above) that presents a material risk of significant harm to an appreciable number of children/adults in the UK (“harm” meaning physical and psychological harm, whether arising from the nature of content or the fact or manner of its dissemination). • Non-priority content is now defined as “content of a kind which presents a material risk of significant harm to an appreciable number of children and adults”. | <p>Anti-competitive behaviour of a large digital group, which as online platforms hold a special and stable market position in the digital economy (“gatekeepers”).</p> <ul style="list-style-type: none"> • DMA sets standards for how the digital economy of the future will function by enforcing fair competition, innovation and more choice for consumers. This includes the freedom and choice to use the core services of Big Tech companies such as browsers, search engines or messaging whilst ensuring that control over data lies with the user. |
| <p>Protection of children</p>  | <p>Safeguards for the protection of minors are included (not published yet).</p> <ul style="list-style-type: none"> • Companies will have to assess and limit the risks their platforms pose to children. • Bans on targeted adverts to children and those based on special characteristics users. | <p>Specific duties if services are likely to be accessed by children.</p> <ul style="list-style-type: none"> • Services will have to carry out a child accessibility assessment to determine: (i) whether it is possible for children in the UK to access the service (or any part of it); and (ii) whether there are a significant number of child users of the service, or (iii) the service is of a kind likely to attract a significant number of child users. • Services will have to have extra systems and processes in place to stop children from coming across harmful content (for example, by using age verification or another means of age assurance). This includes conducting a child safety risk assessment (which requires separate consideration of children in different age groups and children who have certain characteristics or are members of a certain group (the specifics of which still remain unclear)), implementing mitigations to protect children, and making certain information available in the terms of service (e.g., how children are prevented from encountering illegal/harmful content and how they are judged to be at risk of harm). • There is also duty on pornography sites to prevent children from access (even if the sites do not contain user-to-user content), for example, by using age verification, and to keep a written record of the measures taken to comply. | <p>Not included.</p> <ul style="list-style-type: none"> • The proposed ban of targeted advertising towards minors by European Parliament was removed on the basis that content moderation issues should instead be tackled by the DSA. |

| | | | |
|--|--|--|---|
| <p>Online advertising</p>  | <p>Included.</p> <ul style="list-style-type: none"> All online platforms will have to adopt measures for transparent online advertising to users and to show certain information, such as who is paying and sponsoring for the displayed ads, the target audience of the advertisements, how and why it targets a user. VLOPs and VLOSEs will 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 and VLOPs will be limited on the use of sensitive personal data for targeted advertising (e.g. to users with special characteristics such as ethnicity, political views, sexual orientation). VLOPs will also be required to keep databases of verified ads, containing historic information as to the content and targeting of advertisements and the total number of recipients reached. This must be kept for 1 year after the advertisement was displayed for the last time. There is an extended list of transparency requirements (for example, 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> <ul style="list-style-type: none"> A paid-for advertisement can now qualify as user-generated content (UGC) and is therefore subject to the various safety duties that apply to such content (i.e. covering illegal content and content harmful to children/adults). Not all paid-for advertisement will qualify as UGC, but may amount to a fraud offence. In this case, it will instead be subject to the new fraudulent advertising safety duties. The provider must use proportionate systems and processes designed to: (i) prevent individuals from encountering content consisting of fraudulent advertisements, (ii) minimise 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. Clear and accessible provisions in the terms of service must also be included, giving information about any proactive technology used to comply with the above duty (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 will be 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; and 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). <p>Gatekeepers will be prohibited from:</p> <ul style="list-style-type: none"> Collecting end-user personal data across multiple platform services without explicit consent (in line with GDPR); and Exploiting their platform data to compete with commercial users services without explicit consent. |
| <p>Cookies</p>  | <p>Included.</p> <ul style="list-style-type: none"> In order to stop manipulating users’ choices through nudging or deceitful techniques, all service providers will be prohibited from using dark patterns (misleading interfaces and practices) to mislead or manipulate users’ choices unless they pertain to practices permitted by the EU GDPR or the Unfair Commercial Practices Directive. The European Commission is expected to issue guidance on the types of practices that constitute dark patterns under the DSA. | <p>Not currently included.</p> | <p>Included.</p> <p>Gatekeepers will be required to:</p> <ul style="list-style-type: none"> Provide tools to end-users to facilitate the exercise of data portability rights, including by the provision of continuous and real-time access to data; Allow end-users to install and effectively use third-party software applications or software applications stored on operating systems of the gatekeeper; and Provide smaller search engine operators with access to anonymized ranking, search, click, and view data on FRAND terms. <p>As with the rules on online advertising, Gatekeepers will be prohibited from:</p> <ul style="list-style-type: none"> Collecting end-user personal data across multiple platform services without explicit consent (in line with GDPR); and Exploiting their platform data to compete with commercial users services without explicit consent. |

Obligations – what do you have to do to comply

Overall duty



No overall duty. Obligations vary depending on the sub-category of service caught but center around four main principles: (i) transparency, (ii) empowering users, (iii) risk management obligations, and (iv) industry cooperation.

- All service providers without an establishment in the EU must appoint a **contact/legal representative** in a member state where they offer services.
- **Businesses may become ‘trusted flaggers’ of illegal content or goods, with special priority procedures and tight cooperation with platforms.**
- **Content targeting victims of cyber violence (e.g., “revenge porn”) must be removed “immediately”; other content deemed illegal must be removed “swiftly”.**
- Online platforms and VLOPs will 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 the compliance with the DSA.** Only annual reports are required for intermediary services.
- **Online platforms and VLOPs 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 market places will help identify sellers of illegal goods or reasonable efforts by online market places to randomly check whether products or services have been identified as being illegal in any official database.**
- Online platforms and VLOPs are also required to display **trader information** to users and vet the credentials of any third-party suppliers (“KYBC”). **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 Online Advertising).**




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. Additional duties also applies to services likely to be accessible by children and Category 1 services.

- Publish annual **transparency reports**. Exactly what should be included, and other details regarding format, submission and publication, is to be defined by Ofcom.
- Set **clear and accessible terms of service** that state how users (including children) are protected from illegal content, and enforce these terms consistently. **The terms of service should separately address terrorism, CSEA and other priority illegal content and should also specify what proactive technology is in place.**
- **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 need documentation to be provided).**



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 will have to open up and **interoperate** with smaller messaging platforms (i.e. allow the exchange of messages, files and calls across messaging apps). Interoperability obligation/provisions for social networks will be assessed in the future.
- Gatekeepers will be required to offer **fair and non-discriminatory terms and conditions** when using online sales platforms for application software. They will 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 difficult.
- Gatekeepers will be 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.

| | | | |
|---|--|---|---|
| <p>User controls and redress</p>  | <ul style="list-style-type: none"> 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. Platforms must provide a statement of reasons when they remove or disable access to specific content. Online platforms and VLOPs must provide content dispute resolutions mechanisms allowing users to challenge platform's content moderation decisions and seek redress, either via an out-of-court dispute mechanism or judicial redress. These platforms will also be required to adopt measures against abusive notices and counter-notices. | <ul style="list-style-type: none"> All services must have systems and processes in place that allow users to report illegal content or legal but harmful content to adults and children, and 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. | <p>Not currently included.</p> <ul style="list-style-type: none"> No user controls or redress but merger control of gatekeepers (see below). |
| <p>Safety, risk management, and reporting requirements</p>  | <ul style="list-style-type: none"> Obligations to remove illegal goods, services or content. Online platforms with hosting services are required to report criminal offences. New 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 analyse 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. In addition, 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. | <ul style="list-style-type: none"> All services must carry out and maintain illegal content risk assessments (with each kind of content separately assessed) and keep a written record of every assessment. Content that is harmful to adults (but not designated by regulation) does not need to be addressed in the risk assessment. 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, minimise the duration of such content and swiftly remove any illegal content). The systems and processes above apply across all areas of a service and, if proportionate, can include design of functionalities, algorithms and other features. The reporting duty covers all content harmful to adults (i.e. not just priority content). All UK service providers must have systems and processes in place that secure (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. | <ul style="list-style-type: none"> 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. Gatekeepers will be 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 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 will be 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 non-confidential summary will also need to be published annually. |
| <p>Record keeping and review</p>  | <ul style="list-style-type: none"> External and independent auditing of their risk management, including for their algorithmic systems. | <ul style="list-style-type: none"> All services must keep written records of risk assessments (in an easily understandable form) and records of any measure taken or in use to comply with its duties (including those recommended in OFCOM codes of practice, as well any alternative measures that are not recommended in the codes of practice and how these demonstrate compliance). The updated OSB 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 children's access assessments, user empowerment, fraudulent advertising, user identity verification, and CSEA content reporting. | <ul style="list-style-type: none"> Currently 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. |

Sanctions and enforcement

| Sanctions and enforcement | | | |
|---|---|--|---|
| <p>Regulator</p>  | <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 will be required to: (i) publish codes of practice (e.g. on terrorism and child exploitation content, and certain recommendations on the use 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 children’s 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"> Commission is 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 includes 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 will be able to empower national competition authorities to start investigations and transmit their findings to the Commission. |
| <p>How will companies be punished?</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. | <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 OSB has extended the list of offences for which a named director can be held liable. The defences available vary depending on the offence committed. OFCOM will begin enforcing against senior executive within two months (rather than two years) of the OSB coming into effect. | <ul style="list-style-type: none"> Fines - up to 10% of a gatekeeper’s total worldwide turnover (20% for a repeat offence). Market Investigation – by the Commission, which could potentially lead to behavioural or structural remedies, if a gatekeeper systematically fails to comply with the DMA (at least three breaches in eight years). |

Exemptions



Freedom of speech.

- Services must mitigate how their content moderation systems impact freedom of expression.

Freedom of speech, privacy and journalistic exemption.

- All services have a duty to protect users' rights to freedom of expression and privacy within the law. **There is a duty to include clear and accessible provisions in the terms of service informing users about their right to bring a claim for breach of contract if content that they generate, upload or share is taken down, or access to it is restricted, in breach of the terms of service. In addition, category 1 service providers must specify in a publically available statement the "positive steps" it has taken to protect against these rights.**
- Category 1 service providers will also be 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 the purposes of applying the terms of service.**
- **Recognised news publishers' content is not in scope of the OSB.**
- **Individuals will have the right to appeal content removal.**

Public interest reasons

- On limited grounds of public health or public security, the Commission will have discretion on whether the obligation apply 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 won't be able to rely on the grounds of exemption based on public morality.

Timeline



- **The European Parliament (EP) and the Council are expected to formally adopt the proposed Regulation without further amendments, following the informal agreement reached on the final text on 23 April 2022 (not yet publicly available).**
- **Once adopted, the DSA will be directly applicable across the EU from the later of 1 January 2024 or fifteen months after entry into force.**
- **VLOPs and VLOSEs engines may need to adhere sooner, as the DSA is expected to apply to them four months after their designation.**

- **The OSB received a second reading in parliament on 19 April 2022, and now in Committee Stage, is expected to be presented back by 30 June, then the OSB becoming law in late 2022. With an implementation period of 6 months, the new duties would be expected to take effect from middle of 2023.**

- Following the provisional agreement on the final text of the DMA by the European Parliament (EP), the EU Commission, and the Council of the EU on 24 March 2022, the next step will be to finalise the agreement at technical level and to formally adopt the Regulation by both the EP and the Council.
- Once this process is complete, the DMA will come into force 20 days after its publication in the EU Official Journal and the rules will apply six months after (expected not before 2023).