OSA vs DSA

TaylorWessing

	Online Safety Act (UK)	Digital Services Act (EU)
Overview		
Overview	■ The objectives of the UK's Online Safety Act (OSA) and the EU's Digital Service Act (DSA) are materially similar – making the internet a safer place for those that access it in the UK and EU, respectively. ■ In attempting to achieve this, both Acts take a safety by design approach and impose tiered obligations, with progressively greater obligations being imposed on high-reach and high-risk providers. Both impose duties around risk assessments, safety and transparency and seek to balance these duties against user's fundamental rights such as the right to freedom of expression within the law. ■ However, there are key differences. The types of service provider and content in scope are different but overlapping. The OSA applies to the those who provide user-generated content and imposes obligations only in relation to such content (where that content amounts to a criminal offence or is harmful to children). Conversely, the DSA applies to all intermediaries and imposes obligations in relation to all types of illegal content (whether that content amounts to a criminal or civil wrong) as well as systemic risks arising from other types of content and activities. There are also significant differences in the detail such as in relation to which services must conduct risk assessments, the nature of the safety and other duties, what must be included in terms of service, and the extent of the obligations relating to children and advertising. ■ With both Acts now in force (although the OSA effectively not yet applying, with some exceptions), we take a **high-level** look at some of the key overlaps and differences that in-scope digital service providers will need to consider under both regimes.	
Services in scope		
Types of service in scope	The OSA applies to providers of **user-to-user services, search services** and pornographic content services which have **links to the UK** and are not **exempt**. ■ **User-to-user services** Internet services by means of which content generated directly on the service by a user, or uploaded or shared on the service by a user, may be encountered by another user(s). ■ **Search services** Internet services that are or include a search engine ie which enable a person to search more than one website or database. The definitions are broader than at first sight and will capture a number of providers, including search engines, databases, content-sharing platforms, social media platforms, online marketplaces, online gaming services, blogs, forums, listings sites and any other sites that allow users to post or share user-generated content. There are transitional provisions for video service providers. Certain obligations apply to all user-to-user and search services. Additional obligations are imposed on **Category 1 and 2 services** (user-to-user and search services that meet certain threshold conditions to be set out in secondary legislation) and **services likely to be accessed by children** (under-18s). Services are likely to be accessed by children where the children's access assessment concludes that: ■ It is possible for children to access the service or a part of it (which will be the case unless age verification or estimation - but not self-declaration of age - is used, with the result that children are not normally able to access that service/part); and ■ There is a significant number of children who are users of the service/part of the service, or the service/part of the service is of a kind likely to attract a significant number of users who are children (the child user condition). The OSA also imposes obligations on certain providers of pornographic content, but they are not covered here. Likewise, obligations on search services (which are similar to those on user-to-user services) are not specifically covered here. For more on who is in scope, see here. For more on the 'likely to be accessed by children' test (including how it compares to ICO guidance), see here.	The DSA applies to providers of any intermediary service (ie a **mere conduit service**, a **caching service** or a **hosting service**), that has a **substantial connection to the EU**. ■ **Mere conduit service** An information society service, consisting of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network. This includes internet exchange points, wireless access points, virtual private networks and DNS services. ■ **Caching service** An information society service, consisting of the transmission in a communication network of information provided by a recipient of the service, involving the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients upon their request. This includes content delivery networks, reverse proxies and content adaptation proxies. ■ **Hosting service** An information society service, consisting of the storage of information provided by, and at the request of, a recipient of the service. This includes cloud computing, web hosting, file sharing and online platform services. These are further split into **online platforms/search engines** and **very large online platforms/search engines (VLOPs and VLOSEs)**. Obligations are tiered such that progressively greater obligations apply to intermediaries that are hosting services, online platforms/search engines and VLOPs/VLOSEs. ■ **Online platforms** A subset of hosting services that, "at the request of a recipient of the service, stores and disseminates information to the public, unless that activity is a minor and purely ancillary feature…". This includes social networks and online marketplaces (but not the comments section in a newspaper). ■ **Online search engines** An intermediary service that allows users to input queries to perform searches of websites on the basis of a query and returns results in which information related to the requested content can be found. This includes web search providers. ■ **VLOPs** 'Very large Online Platforms' that have at least 45 million average monthly active users/recipients within the EU and are designated as such by the European Commission. ■ **VLOSEs** 'Very large Online Search Engines' that have at least 45 million average monthly active users/recipients within the EU and are designated as such by the European Commission. For more on who is in scope, see here.

OSA vs DSA

TaylorWessing

	Online Safety Act (UK)	Digital Services Act (EU)
Territory	A service has **links with the UK** if (i) it has a significant number of users in the UK, (ii) it is targeting UK users, or (iii) the service is capable of being used in the UK and there are reasonable grounds to believe that the user generated content presents a material risk of significant harm to individuals in the UK.	**A substantial connection** to the EU means a substantial connection arising from the service provider's establishment in the EU or other specific factual criteria such as the provider having a significant number of users in one or more Member State, or the targeting of activities towards at least one Member State. In the future the DSA will also apply to all EEA countries.
Exemptions	Certain service providers are **exempt**. These include providers of certain communication services (eg emails, SMS messages, MMS messages and one-to-one live aural communications), limited functionality services (those who only have "below the line" content), and certain providers of education and childcare. There are similar exemptions for parts of services and content of the above kinds. All exemptions are drafted narrowly. If a service or part of a service has regulated user-generated content that does not fall within an exemption, then the obligations under the OSA will apply to that content.	Not applicable – the DSA does not include an explicit provision on exemptions. However, micro and small enterprises are exempt from some obligations and have had more time (than larger businesses) to implement others.
Content in scope		
Content in scope	The OSA applies to regulated user-generated content. Content means anything that can be communicated by means of an internet service whether publicly or privately (including where automatically generated), subject to exclusions. Content in scope is further classified as: ■ **Illegal content** – any word, image, speech, or sound that amounts to a **relevant offence**. A **relevant offence** is either: (i) a **priority offence** – offences relating to: (a) terrorism; (b) child sexual exploitation and abuse content (CSEA content); and (c) other priority offences specified in schedule 7; or (ii) Any other offence where the intended victim is an individual(s); and the offence is not considered to be a priority offence. Subject to **exclusions** including for: infringement of intellectual property rights; the safety or quality of goods; the performance of a service by a person not qualified; and offences under certain consumer protection legislation. ■ **Content that is harmful to children**. The OSA identifies three types of such content: (i) **primary priority content that is harmful to children** – pornographic content, content encouraging, promoting or instructing on suicide, deliberate self-injury or eating disorders/behaviours; (ii) **priority content that is harmful to children** – bullying content or content which (a) is abusive and targets race, religion, sex, sexual orientation, disability or gender reassignment; (b) incites hatred against people based on these characteristics; (c) encourages/promotes/instructs on serious violence against a person or a challenge/stunt likely to result in serious injury; (d) depicts serious violence or (in graphic detail) serious injury against a person/animal/fictional creature; (e) encourages self-administration of physically harmful substances; and (iii) content that is not covered by (i) or (ii), but is of the kind which is considered to present a **material risk** of **significant harm** to an **appreciable number of children in the UK**. Category 1 services also have additional obligations regarding adult user content. This is content which (a) encourages/promotes/instructs on suicide, deliberate self-injury or eating disorders/behaviours (b) is abusive (and targets race, religion, sex, sexual orientation, disability or gender reassignment) or (c) incites hatred against people based on the aforementioned characteristics. The obligations therefore do not apply to any regulated user-generated content that constitutes a civil wrong. For more on how service providers will need to make judgments about whether content is illegal content or harmful to children, see here.	Many of the obligations in the DSA apply to **illegal content** – any 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 any Member State (which is in compliance with Union law), irrespective of the precise subject matter or nature of that law. This could include content that constitutes a criminal or civil wrong. Some provisions also relate to content prohibited by service providers' terms of service. Obligations on VLOPs and VLOSEs extend to **systemic risks** (which go beyond illegal content) – see the sections on risk assessments and safety duties below.

OSA vs DSA

TaylorWessing

	Online Safety Act (UK)	Digital Services Act (EU)
Duties		
Risk assessments	■ **All** user-to-user service providers must conduct (a) an illegal content risk assessment and (b) a children's access assessment to determine whether it is possible for children to access all or part of a service and whether the child user condition is met – this will determine if additional obligations concerning content that is harmful to children apply. ■ Providers of **Category 1** services must conduct an adult user empowerment risk assessment relating to **adult user content**. ■ Providers of **services likely to be accessed by children** must conduct a children's risk assessment. There are provisions relating to when risk assessments must be first undertaken and repeated. For more on risk assessments, see here.	**VLOPs and VLOSEs** must produce an annual assessment of the systemic risks stemming from the design, functioning and use of their services and related systems (including algorithmic systems) in relation to: (i) The dissemination of illegal content. (ii) Any actual or foreseeable negative effects for the exercise of fundamental rights. (iii) Any actual or foreseeable negative effects on civic discourse and electoral processes, and public security. (iv) Any actual or foreseeable negative effects in relation to gender-based violence, the protection of public health and minors and serious negative consequences to the person's physical and mental well-being. There are provisions relating to when risk assessments must be first undertaken and repeated.

OSA vs DSA

TaylorWessing

	Online Safety Act (UK)	Digital Services Act (EU)
Safety duties	■ **All** service providers must: (i) Take or use proportionate measures relating to the design or operation of the service to (a) prevent individuals from encountering priority illegal content, (b) effectively mitigate and manage the risk of the service being used for the commission or facilitation of a priority offence as identified in the risk assessment, and (c) effectively mitigate and manage the risk of harm from illegal content to individuals as identified in the risk assessment. (ii) Use proportionate systems and processes to (a) minimise the length of time priority illegal content is present and (b) swiftly take down any illegal content when alerted / made aware. ■ Providers of **Category 1** services must (i) implement proportionate features to allow adult users to reduce the likelihood of encountering (or alert the user to the possibility of encountering) adult user content ('control features') and (ii) offer all adult users the opportunity to verify their identity and include features allowing adult users to filter out non-verified users. They also must not act against users except in accordance with their terms of service. ■ Providers of **services likely to be accessed by children** must: (i) Take or use proportionate measures relating to the design or operation of the service to effectively mitigate and manage the risks (and impact) of harm to children in different age groups as identified in the risk assessment. (ii) Use proportionate systems and processes to prevent children from encountering primary priority content that is harmful to children, including by using age verification and assurance, and protect children in age groups judged to be at risk of harm from encountering other content that is harmful to children. For more on safety duties, see here, and on all the duties as they relate to children, see here.	■ **All** service providers must: (i) Upon receipt of an **order** to act against specific items of illegal content (or to provide specific information) issued by the relevant national judicial or administrative authority, inform the authority of any effect given to the order without undue delay, specifying if and when effect was given to the order. (ii) Inform the recipient of the service concerned of the order received and the effect given to it, including a statement of reasons, the possibilities for redress that exist, and a description of the territorial scope of the order. (iii) Act in a diligent, objective and proportionate manner in applying and enforcing **restrictions they impose in relation to the use of their service**, with due regard to the rights and legitimate interests of all parties involved, including the fundamental rights of the recipients of the service, such as freedom of expression, freedom and pluralism of the media, and other fundamental rights and freedoms as enshrined in the Charter. ■ **Hosting service providers** must put in place **notice and action** mechanisms for illegal content. Confirmation of receipt must be provided as well as the decision in respect of the information and the possibility of redress. Decisions must be taken in a timely, diligent, non-arbitrary and objective manner and if automated means are used, information must be provided. In certain circumstances, hosting service providers must also provide a clear and specific statement of reasons to affected users as to why the service provider took action in relation to an order to act against illegal content or to provide information. ■ **Online platforms** must: (i) Give priority to notices received from "trusted flaggers" (bodies certified as having particular expertise in identifying and notifying illegal content). (ii) Suspend provision of their service to users who frequently provide manifestly illegal content and suspend the processing of notices and complaints through the notice and action mechanisms for submitters of manifestly unfounded notices or complaints. (iii) Not design, operate or organise their interfaces "in a way that deceives, manipulates or otherwise materially distorts or impairs the ability of recipients of their service to make free and informed decisions" (sometimes called dark patterns). (iv) Put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors (for platforms accessible to minors). ■ **VLOPs and VLOSEs** must: (i) Put in place reasonable, proportionate and effective mitigation measures tailored to the specific systemic risks identified in the risk assessment (see above and note that these go beyond illegal content). (ii) Submit to independent audits. (iii) Establish an independent compliance function. (iv) Provide at least one option for each recommender system not based on profiling. (v) Comply with any Commission decision setting out specific measures in times of crisis, aimed at preventing, eliminating or limiting any contribution to identified serious threats. Liability/safe harbour provisions closely similar to those in the e-Commerce Directive are also included in the DSA. For more on safety duties, see here, on duties in general, see here and on dark patterns and recommender systems, see here.

OSA vs DSA

TaylorWessing

	Online Safety Act (UK)	Digital Services Act (EU)
Terms of service	■ **All** service providers must specify (i) how individuals are to be protected from illegal content including any proactive technology used, (ii) users' rights to bring claims for breach of contract in certain circumstances and (iii) policies and processes for the handling of different kinds of complaints. ■ **Providers of services likely to be accessed by children** must specify (i) how the children's safety duties are to be met and any proactive technology used, (ii) details of any measures used to prevent children accessing the service or any part of it and (iii) that primary priority content is prohibited for all users (unless age verification/estimation is used). ■ Providers of **Category 1 services** must (i) summarise the findings of the most recent illegal content risk assessment and adult user empowerment risk assessment, (ii) specify details of control features offered and how users can take advantage of them, (iii) specify various information about protecting content of democratic importance and about journalistic content and (iv) specify details of any proactive technology used to combat fraudulent advertising and (v) specify how identity verification works. Providers of Category 1 services must not act against users except in accordance with their terms of service. ■ Providers of **Category 1 services likely to be accessed by children** must summarise the findings of the most recent children's risk assessment. ■ Providers of **Category 1 and 2 services** must specify their approach to deceased child users and comply with them. There are also various provisions requiring certain terms of service to be clear, accessible (in some cases including to children), transparent and applied consistently. For more on terms of service, see here.	■ **All** service providers must set out: (i) Any restrictions that they impose in relation to the use of their service, including any policies on content moderation (including algorithmic decision-making and human review), as well as the rules of procedure of any internal complaint handling system. (ii) The conditions for, and any restrictions on, the use of the service in a way that minors can understand (where a service is primarily directed at minors or is predominantly used by them). ■ **VLOPs and VLOSEs** must provide users with a concise, easily accessible, and machine-readable summary of their terms of service, including the available remedies and redress mechanisms, in clear and unambiguous language and publish their terms of service in all official languages of the EU Member States in which they offer their services.

OSA vs DSA

TaylorWessing

	Online Safety Act (UK)	Digital Services Act (EU)
Transparency		
Record keeping, review and reporting	■ **All** service providers must keep written records of (i) risk assessments (including how they were carried out and the findings) and (ii) measures taken to comply with duties and reasons for using methods not in codes of practice. They must also review compliance with duties regularly and after making significant changes to any aspects of the service's design or operation. ■ Providers of **Category 1 services** must (i) keep written records of adult user empowerment risk assessments (including how they were carried out and the findings) and (ii) supply copies of all of their risk assessments (illegal content, children's and adult user empowerment) to OFCOM. Providers of **Category 1 and 2 services** must also produce an annual transparency report containing information required by Ofcom. For more on record keeping and review, see here.	■ **All** service providers must make publicly available yearly reports on (i) content moderation undertaken including the number of orders received from authorities, (ii) any content moderation undertaken at the providers own initiative, (iii) the number of complaints received through internal complaint-handling systems in accordance with the providers terms of service, (iv) any use of automated means of content moderation and (v) various related information. They must also designate and publish a single point of contact for communication with authorities and users of the service in the EU (plus the relevant language of communication). ■ **Hosting services** must make publicly available yearly reports on notices submitted by recipients and trusted flaggers, the action taken, on what basis, within what timeframe, and any use of automated means. ■ **Online platforms** must make publicly available yearly reports on (i) the number of disputes submitted to the out-of-court dispute settlement bodies, their outcomes, time taken for resolution, and compliance with decisions, (ii) additional issues around complaints received through the internal complaints-handling mechanism, (iii) information regarding user suspensions, (iv) the average number of monthly active EU users (every six months), (v) certain statements of reasons and (e) the main parameters used in recommender systems and options to modify them. ■ **VLOPs and VLOSEs** must (i) submit to annual independent audits, (ii) provide requested data to authorities and researchers and (iii) report on/publish (a) enhanced information regarding advertisements and advertisers, and human content moderation functions, (b) risk assessments, mitigation measures and audits and (c) the average number of monthly active users in each Member State. VLOPs must also specify information regarding resources and other information applied to content moderation. There are various additional record keeping and review obligations. For more on reporting obligations, see here, and on recommender systems, see here.
Content reporting and complaints	■ **All** service providers must (i) use systems and processes that allow easy reporting of illegal content by users and affected persons and (ii) operate an easy to access and use complaints procedure that allows for complaints about illegal content, compliance by services with safety and other duties, take downs, user sanctions and use of proactive technology. ■ Providers of **services likely to be accessed by children** must (i) use systems and processes that allow easy reporting of content that is harmful to children (present on a part of the service that it is possible for children to access) by users and affected persons and (ii) operate an easy to access and use complaints procedure that allows for complaints about content that is harmful to children, compliance by services with children's safety duties, take downs, user sanctions and incorrect age assessments. ■ Providers of **Category 1 services** must operate an easy to access and use complaints procedure which allows complaints about user empowerment, content of democratic importance, news publisher content, journalistic content and freedom of expression and privacy. There are additional duties about news publisher content.	■ **All** service providers must provide a statement of reasons to affected users as to why they took action in relation to an **order** to act against specific items of illegal content (or to provide specific information) issued by the relevant national judicial or administrative authority. See also the safety duties above. ■ **Hosting services** must follow prescriptive requirements for communications with a notice submitter and any affected users, including giving specific reasons to affected users if certain restrictions are imposed (on the grounds that the content is illegal content or prohibited under the service provider's terms of service) and details of the means of redress. See also the safety duties above. ■ **Online platforms** must put in place an effective internal complaint-handling system for content moderation decisions, provide reasoned decisions on any such complaints and engage with certified out of court settlement dispute bodies. Decision must not be solely based on automated means. See also the safety duties above.
User redress	The principal method of redress for users is a breach of contract claim (breach of the terms of service) – service providers are required to inform users about their right to bring a breach of contract claim if their content is taken down, or access restricted to it.	The principal method of redress for users of **online platforms** is to use a certified out-of-court dispute settlement body to resolve content moderation and service suspension disputes. Users can also bring a breach of contract claim before the courts against intermediaries.

OSA vs DSA

TaylorWessing

	Online Safety Act (UK)	Digital Services Act (EU)
Advertising		
Advertising	Providers of **Category 1 and 2A services** must put in place proportionate systems and processes designed to prevent individuals from encountering fraudulent adverts on the service, minimise the length of time such content is present, and swiftly take such content upon becoming aware of it.	■ **Online platforms** must take steps to identify ads, the advertiser, and information about the parameters used to determine who the ad is presented to and how to change that (Ad Information). They must not present ads to users based on profiling using special categories of personal data (all users) or personal date (minors). There are also disclosure requirements relating to advertising. ■ **VLOPs** must maintain a repository of Ad Information for a period of one year after the ad was last presented. For more on advertising, see here.
Freedom of speech and journalistic content		
Freedoms	■ **All** service providers are required to have regard to the importance of protecting (i) user's right to freedom of expression within the law and (ii) users from unlawful breaches of privacy. ■ Providers of **Category 1 services** have duties to protect content of democratic importance, news publisher content and journalistic content. They must assess the impact of safety measures and policies on freedom of expression and privacy and the availability/treatment of news publisher content and journalistic content, as well as publish and keep such impact assessments up to date. For more on protecting fundamental rights and freedoms, see here.	■ When applying restrictions on use in their terms, **all service providers** must consider the rights and legitimate interests of all parties involved, including the fundamental rights of users, like freedom of expression, freedom and pluralism of the media, and other fundamental rights and freedoms as enshrined in the Charter. ■ **VLOPs** must consider actual or foreseeable negative effects of the exercise of fundamental rights (including freedom of expression and the freedom and pluralism of the media) as part of their annual systemic risk assessments.
Enforcement and sanctions		
Enforcement	■ OFCOM is the regulator which will oversee the regime. It must produce codes of practice relating to nearly all duties, which will include how the duties can be met. ■ Various new offences have been created under the OSA, such as failure to comply with an information notice. Under these offences senior managers, parent entities and subsidiaries may be liable in certain circumstances. ■ Ofcom is given wide-ranging enforcement powers including the ability to issue fines of up to 10% of annual global turnover or £18m (whichever is greater) and to obtain various business disruption measures. For more on Ofcom's powers and duties under the OSA, see here, and on Ofcom's three-year plan to regulate the OSA, see here.	■ Regulation is by the Digital Services Co-ordinator in the member state of establishment and (in the case of VLOPs and VLOSES), the European Commission. Various entities are already under investigation. Fines of up to 6% of the annual worldwide turnover can be imposed for infringements. This maximum is reduced to 1% of the annual income or worldwide turnover for certain information offences, and 5% for periodic penalty payments. For more on national enforcement, see here.
Other notable requirements		
Other	■ Under the DSA, online platforms must conduct KYC checks on traders that conclude distance contracts with consumers on the platform, design interfaces to allow traders to comply with obligations towards consumers and inform consumers on awareness of illegal products and services. For more on KYC obligations, see here. ■ Under the DSA, providers of hosting services must notify law enforcement of suspicion of criminal offences involving threat to life or safety of persons. The OSA imposes certain duties on all service providers about reporting CSEA content to the NCA. ■ The OSA contains various provisions about deceased child users and the provision of information by service providers to authorities in relation to the investigation into the death of a child user.	

Our team

Mark Owen
Partner
+44 20 7300 4884
m.owen@taylorwessing.com

Adam Rendle
Partner
+44 20 7300 4787
a.rendle@taylorwessing.com

Xuyang Zhu
Senior Counsel
+44 20 7300 7000
x.zhu@taylorwessing.com

Timothy Pinto
Senior Counsel
+44 20 7300 7000
t.pinto@taylorwessing.com

Louise Popple
Senior Counsel
+44 20 7300 4787
l.popple@taylorwessing.com

Debbie Heywood
Senior Counsel
+44 20 7300 7000
d.heywood@taylorwessing.com

Our locations

2000+ people
1200+ lawyers
300+ partners
28 offices
17 jurisdictions

Argentina*	Buenos Aires	**Mexico***	Mexico City
Austria	Klagenfurt | Vienna	**Netherlands**	Amsterdam | Eindhoven
Belgium	Brussels	**Nicaragua***	Managua
Brazil*	Belo Horizonte | Brasilia | Rio de Janeiro | São Paulo	**Panama***	Panama City
Chile*	Santiago de Chile	**Poland**	Warsaw
China	Beijing | Hong Kong | Shanghai	**Portugal***	Braga | Lisbon | Porto
Colombia*	Bogotá | Bogotá, main office	**Puerto Rico***	San Juan
Costa Rica*	Guanacaste | San José	**Republic of Ireland**	Dublin
Czech Republic	Brno | Prague	**Slovakia**	Bratislava
Dominican Republic*	Santo Domingo	**South Korea****	Seoul
Ecuador*	Cuenca | Guayaquil | Manta | Quito	**Spain***	Barcelona | Canary Islands | Madrid | Pamplona | Seville | Valencia | Vitoria | Zaragoza
El Salvador*	San Salvador	**UAE**	Dubai
France	Paris	**Ukraine**	Kyiv
Germany	Berlin | Düsseldorf | Frankfurt | Hamburg | Munich	**United Kingdom**	Cambridge | Liverpool | London
Guatemala*	Guatemala	**Uruguay***	Montevideo
Honduras*	San Pedro Sula | Tegucigalpa	**USA**	New York | San Francisco
Hungary	Budapest		

* Powered by our strategic alliance with leading law firm ECIJA
** In association with DR & AJU LLC