The UK's OSA vs the EU's DSA: how similar are they?

TaylorWessing

	Online Safety Act	Digital Services Act
Services in scope		
Types of service in scope	■ **User-to-user services** Internet services which allow content generated, uploaded or shared by a user to be encountered by another user(s). Category 1 and 2B user-to-user services that meet certain threshold conditions to be set out by the Secretary of State following advice from Ofcom. ■ **Search services** Internet services that allow users to search more than one website or database. **While many obligations relate to all in-scope services there are additional obligations on:** ■ **User-to-user and search services likely to be accessed by children** Services that are possible for children to access and meet the "child user condition" (i.e. there are a significant number of children who are users of the service; or the service is likely to attract a significant number of users that are children). ■ **Category 1, 2A and 2B services and combined services** Ofcom will outline the relevant thresholds for these categories once the Secretary of State makes a regulation specifying the relevant conditions to be met.	■ **Mere conduit services** e.g. Internet exchange points, wireless access points, virtual private networks and DNS services. ■ **Caching services** e.g. Content delivery networks, reverse proxies and content adaptation proxies. ■ **Hosting services** e.g. Cloud computing and web hosting services. ■ **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…" e.g. social networks and online marketplaces. ■ **Online search engines** an intermediary service that allows users to input queries to perform searches of websites and returns results in which information related to the requested content can be found e.g. 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.

	Online Safety Act	Digital Services Act
	which: ■ have links with the UK – i.e. the service has a significant number of users in the UK, is targeting UK users, or 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; and ■ is **not exempt** (see below).	**which:** ■ have a **substantial connection** to the EU – i.e. the service provider is either established in the EU, has a significant number of users in a Member State, or targets at least one Member State. ■ In the future the DSA will also apply to all EEA countries.
Exemptions	■ The OSA makes certain services exempt, these include providers of certain communication services (e.g. providers of emails, SMS, MMS services) and providers of education or childcare.	■ Not applicable – the DSA does not include an explicit provision on exemptions. But micro and small enterprises are exempt from some obligations and have more time (than larger businesses) to implement others.
Content in scope		
Content in scope	The OSA applies to user-generated content. Content means anything that can be communicated by means of an internet service (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** being, either: (i) a **priority offence** – offences relating to: (a) terrorism; (b) child sexual exploitation and abuse content (CSEA content); and (c) other specified priority illegal content mentioned in schedule 7; or (ii) Any other offence where the intended victim is an individual; 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 consumer protection.	The DSA applies 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 illegal.

	Online Safety Act	Digital Services Act
	■ **Content that is harmful to children**. The OSA identifies three types of harmful content: (i) **primary priority content that is harmful to children** – pornographic content, content encouraging 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), nor (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**.	
Duties		
Risk assessments	■ **All** user-to-user service providers must conduct an illegal content risk assessment. They must also carry out a child access assessment to determine whether it is possible for children to access all or part of a service – this will determine if provisions concerning content that is harmful to children apply. ■ Providers of **Category 1** services must conduct an adult user empowerment risk assessment. ■ Providers of **services likely to be accessed by children** must conduct a children's risk assessment.	■ **VLOPs** and **VLOSEs** must produce an annual assessment of the systemic risks stemming from the design, functioning and use of their services in relation to the dissemination of illegal content (among other considerations), and to implement proportionate measures to mitigate identified risks. ■ Ad hoc risk assessments are required prior to the deployment of functionalities that are likely to have a critical impact on the risks identified in the annual assessment. ■ **All** service providers must take steps against specific illegal content (if they are aware of it or it is brought to their attention), including to take it down, and provide information, upon order of national authorities.

	Online Safety Act	Digital Services Act
Safety duties	■ **All** service providers must: (i) Take or use proportionate measures relating to the design or operation of the service to prevent individuals from encountering priority illegal content, effectively mitigate and manage the risk of the service being used for the commission or facilitation of a priority offence, effectively mitigate and manage the risk of harm (from illegal content). (ii) Use proportionate systems and processes to minimise the length of time priority illegal content is present and swiftly take down any illegal content when alerted/made aware. (iii) Specify in terms of service how individuals are to be protected from illegal content including any proactive technology used; ensure these provisions are clear and accessible; apply the terms of service consistently; summarise findings of most recent illegal content risk assessment and children's risk assessment in terms of service. ■ Providers of **Category 1** services must 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. These features must be easy to access, brought to users' attention and explained in terms of service. ■ Providers of **services likely to be accessed by children** must implement proportionate systems and processes to: (a) effectively mitigate and manage the risks (and impact) of harm to children in different age groups (as identified in the risk assessments); and (b) 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. Risks of harm to children identified in risk assessments must be managed and mitigated. Use of technology must be provided in the terms of service, which must be applied consistently.	■ **Hosting service providers** must put in place notice and action mechanisms for illegal content – these are similar to the e-Commerce Directive requirements. ■ **Online platforms** must give priority to notices reived from "trusted flaggers" (bodies certified as having particular expertise in identifying and notifying illegal content). ■ **VLOPs** and **VLOSEs** must implement reasonable, proportionate and effective mitigation measures tailored to the specific systemic risks identified. In times of crisis, VLOPs and VLOSEs may be subject to specific measures, as laid down in a Commission decision, aimed at preventing, eliminating or limiting any contribution to identified serious threats.

	Online Safety Act	Digital Services Act
Terms of service	■ **All** service providers must set out in their terms of service how individuals are to be protected from applicable content and harms and their policy regarding deceased child users. They must also summarise the findings of their illegal content risk assessments in their terms of service. ■ Providers of **Category 1 services** and **services likely to be accessed by children** have additional obligations relating to publication of risk assessments and the way in which they use technology to deliver their obligations. The terms of service must be clear, transparent and applied consistently.	■ **All** service providers must set out content restrictions, policies and processes in their terms of service and enforce these diligently, objectively and proportionately. ■ **VLOPs** and **VLOSEs** must publish their terms of service in all official languages of the EU Member States in which they offer their services.
Transparency		
Reporting and record keeping	■ Providers of **Category 1 and 2 services** must produce an annual transparency report containing information required by Ofcom. ■ There are various record-keeping and review requirements across all service providers. In many cases these records need to be supplied to Ofcom.	■ **All** service providers must report on the number of orders received from authorities; actions taken; the number of complaints and any use of automated means of content moderation; and other information on content moderation. ■ **Online platforms** must report on: (i) the number of out-of-court disputes, their outcomes, time taken for resolution, and compliance with decisions. (ii) information regarding user suspensions; (iii) the average number of monthly active EU users (every six months); and (iv) the main parameters used in recommender systems and options to modify them. ■ **VLOPs** musty report on: (i) Enhanced information regarding advertisements and advertisers, and human content moderation functions; (ii) risk assessments, mitigation measures and audits; and (iii) the average number of monthly active recipients in each Member State.

	Online Safety Act	Digital Services Act
Complaints	■ **All** service providers must put in place a complaints procedure in which users and news publishers affected by takedown/moderation decisions are able to challenge them.	■ **Online platforms** must put in place a complaints-handling system for content moderation decisions.
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 to it restricted.	■ 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.
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 down upon becoming aware of it.	■ **Online platforms** must take steps to identify adverts, the advertiser, and information about the parameters used to determine who the ad is presented to and how to change that (Ad Information). ■ **VLOPs** must maintain a repository of Ad Information for a period of one year after the ad was last presented.
Freedom of speech and journalistic content		
	■ **All** service providers are required to have regard to the importance of protecting freedom of speech and users' rights to privacy. ■ Providers of **Category 1 services** have duties to protect content of democratic importance, news publisher content and journalistic content. They must also conduct various impact assessments.	■ 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 charter fundamental rights and freedoms. ■ **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.

	Online Safety Act	Digital Services Act
Enforcement and sanctions		
Enforcement and sanctions	■ 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, fellow subsidiaries and controlling individuals 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).	■ Any competent EU Member State (and the Commission alone in the case of VLOPs and VLOSEs) may impose fines of up to 6% of the annual worldwide turnover 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. See here for more information.
Other notable requirements under DSA not covered in the OSA		
	■ **All service providers** must: (i) appoint a contact for communication with authorities and a point of contact for users of the services; and (ii) provide a statement of reasons why they took action in relation to content or the user's activities, including removing content or suspending use of the service. ■ **Online platforms** must: (i) avoid using dark patterns. They are prohibited from designing, operating or organising 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."; and (ii) publish the parameters used in their recommender systems. ■ **VLOPs** must: (i) comply with various crisis response obligations, should the functioning and use of their services significantly contribute to extraordinary circumstances leading to a serious threat to public security or public health in the EU or a significant part of it; and (ii) publish details of how users can turn off recommender systems based on profiling.	