LEWIS SILKIN

Comparison between the Digital Services Act and the Online Safety Act 2023

November 2023

LEWIS SILKIN

The Online Safety Act ("**OSA**") recently received Royal Assent and is likely to come into force in late 2024. The Digital Services Act ("**DSA**") comes into force in EU member states, as well as the EEA in early 2024. Each Act is extra-territorial in effect and will apply to businesses with UK users (Online Safety Act) or EU users (Digital Services Act), wherever in the world those businesses might be located.

Where do these regimes overlap and where do they differ? How can businesses within scope create a compliance strategy that covers both Acts? This table aims to help provide a starting point.

As we do not yet know the full picture under the OSA, this table will be updated as the detailed requirements of the Online Safety Act are developed in secondary legislation and codes of practice to be published in the coming months by Ofcom, the UK's regulator for the OSA. This table is correct as of 9 November 2023.

	Digital Services Act	Online Safety Act
Who comes within scope of each piece of legislation?	The DSA governs intermediary services provided to service recipients (whether businesses or consumers) established or resident in an EU member state, irrespective of where the service provider is established. Intermediary services include mere conduit services, caching services and hosting services. Micro and small businesses are exempt from some requirements and will have more time than larger organisations to implement the other requirements.	Providers of regulated services which include user-to-user and search services and pornographic services. A user-to-user service means an internet service that allows content generated directly on the service, or uploaded to or shared on the service, by a user, to be encountered by another user, or other users. A search service is a service that is or includes a search engine. If outside the UK, services are in scope if they target UK users or have a significant number of UK users. Certain services are exempt, such as providers of certain communication services (e.g., emails, SMS and MMS services) and providers of education or childcare.
	Very large online platforms (VLOPs) and very large online search engines (VLOSEs) have the most obligations. Every six months, online platforms must report on their average monthly active service recipients, so that the European Commission can assess if they should be designated a VLOP or VLOSE. The European Commission has designated some platforms as VLOPs or VLOSEs, including among others Instagram, Facebook, Google Play, Google Maps, X/Twitter, LinkedIn, Wikipedia, Bing and Google Search.	Services are categorised. Category 1 services have additional duties compared to Category 2 services. Whether a service is a Category 1 or Category 2 service will depend on whether they reach "threshold conditions". These will be set out in secondary legislation. Category 1 services are intended to be the larger, more popular sites, that is, those with a higher number of users. Functionality will also be relevant. Ofcom has consulted on how to categorise providers so that it can advise government. It has asked how platforms measure user numbers on different parts of their services.

	Digital Services Act	Online Safety Act
What content is covered?	"Illegal content" is information which is itself illegal or relates to an illegal activity. Examples include the sharing of images depicting child sexual abuse, the sale of products or the provision of services in breach of consumer protection law, and the illegal sale of live animals. Legal but harmful content (for example, relating to bullying or self-harm) is not defined, nor subject to obligations to remove.	Illegal content is content that amounts to an offence specified in one of the schedules, as follows: - A terrorism offence (Schedule 5). - A child sexual exploitation and abuse (CSEA) offence (Schedule 6). - Priority offences (Schedule 7). These include offences such as the sale of illegal drugs or weapons. Harm means physical or psychological harm. The intention is for the OSA to tackle harm to individuals rather than to wider society. What constitutes content that is harmful to children and content that is harmful to adults will be defined in secondary regulations.
What are the duties around risk assessments?	All service providers must employ measures to deal with specific illegal content (if they are aware of it or it is brought to their attention). This includes taking it down or providing information, if national authorities so order. VLOPs and VLOSEs must produce an annual assessment of the systemic risks resulting from the design, functioning and use of their services regarding the dissemination of illegal content and use proportionate measures to mitigate identified risks. They must carry out ad hoc risk assessments before they adopt functionalities that are likely to have a significant effect on the risks identified in the annual assessment.	User-to-user service providers must conduct a risk assessment about illegal content. In addition, they must conduct a child access assessment to see if children can access all or part of a service. If so, they must also conduct a children's risk assessment. A service must notify Ofcom of the presence of content harmful to children. Ofcom has published guidance on a four step process to do this. Category 1 services must also conduct an adult user empowerment risk assessment.

	Digital Services Act	Online Safety Act
What other duties fall on in-scope services?	Hosting service providers must put in place notice and action mechanisms for illegal content. Online platforms must give priority to notices reived from “trusted flaggers” (bodies certified as having 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. 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. There are more extensive reporting obligations on online platforms, and more extensive again for VLOPs. Online platforms must put in place a complaints-handling system for content moderation decisions. Users can employ a certified out-of-court dispute settlement body to resolve content moderation and service suspension disputes.	User-to-user services must 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 to commit or facilitate a priority offence and effectively mitigate and manage the risks of harm to individuals, as identified in the most recent illegal content risk assessment. Providers must also use proportionate systems and processes designed to minimise the length of time for which any priority illegal content is present; and once it knows about illegal content, must take it down swiftly. They must also: - set out in their terms of service how individuals are to be protected from illegal content; - apply their terms of service consistently; - include terms giving information about any proactive technology used by a service for compliance purposes; and - ensure that the terms of service are clear and accessible. All providers must have systems and processes that allow users to easily report illegal content. They must also have complaints procedures for users and news publishers affected by takedown/moderation decisions to challenge the decisions concerned. Users can seek redress via a breach of contract claim (for breach of the terms of service) and so providers must tell users about their right to bring a breach of contract claim if their content is taken down, or access to it is restricted. Service providers must keep records which may be seen by Ofcom, and providers of Category 1 and 2 services must provide an annual transparency report to Ofcom.

	Digital Services Act	Online Safety Act
What does the legislation say about freedom of speech?	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.	When deciding on and implementing safety measures and policies, providers must have regard to the protection of users' right to freedom of expression within the law and users' privacy. Category 1 services must protect content of democratic importance, news publisher content and journalistic content. They must also conduct various impact assessments.
How are the two pieces of legislation going to be enforced?	National Digital Services Coordinators have the power, for providers within their jurisdiction, to investigate suspected infringements (including by on-site inspections), accept compliance commitments and make them binding, order the cessation of infringements and impose fines for non-compliance. Fines are calculated as follows: - For non-compliance generally, the cap is 6% of the intermediary service provider's annual worldwide turnover in the preceding financial year. - For non-co-operation with investigations, the cap is 1% of the intermediary service provider's annual worldwide turnover in the preceding financial year. - Periodic penalty payments, capped at 5% of the intermediary service provider's average daily turnover. Where fines are ineffective, the Digital Services Coordinator can request the competent judicial authority to temporarily restrict access to the service for an extendable period of four weeks. Enforcement against VLOPs and VLOSEs is led by the Commission under specified procedures.	Ofcom can issue fines of £18 million or 10% of global annual turnover, whichever is higher, for breaches of the OSA. It will be able to consider taking enforcement action, which may include business disruption measures, against any in-scope company worldwide that provides services to UK users. Ofcom may issue a notice requiring regulated user-to-user and search services to use accredited technology to identify terrorism and child abuse content and to swiftly take down any such content identified. Ofcom will also have the power to require a company to use best endeavours to develop or source technology to prevent, identify and remove child abuse content.

	Digital Services Act	Online Safety Act
How does the legislation affect advertising?	Online platforms that display advertisements on their online interfaces must ensure that the service recipients can identify, for each specific advert displayed to each individual recipient, in a clear and unambiguous manner and in real time: - That the information displayed is an advert. - The natural or legal person on whose behalf the advertisement is presented and, if different, the person who paid for the advertisement. - Meaningful information directly and easily accessible from the advertisement about the main parameters used to determine the recipient to whom the advertisement is presented and, where applicable, about how to change those parameters. Online platform providers cannot target advertisements at service recipients based on profiling which uses special categories of personal data. Minors may not be targeted with advertisements. Online platform providers must provide service recipients with a functionality to declare whether the content they provide is or contains a commercial communication. If a service recipient uses this functionality, the platform provider must ensure that other service recipients can identify that the content is or contains a commercial communication. Targeting using special category data is prohibited. Providers of online consumer marketplaces must tell consumers if they become aware that a product that they have bought is illegal: either directly if they have contact details or on their website.	Chapter 5 of Part 3 imposes duties on providers of certain regulated user-to-user and search services relating to paid-for fraudulent advertising. Category 1 services will need to put in place proportionate systems and processes to: - Prevent individuals from encountering fraudulent adverts. - Minimise the length of time for which fraudulent adverts are present. - Promptly take fraudulent adverts down once they know about them. Category 2A services (regulated search services or combined services) must use proportionate systems and processes to minimise the risk of individuals encountering fraudulent adverts in or via search results. Regarding what is proportionate, the nature and severity of the potential harm posed by the adverts is relevant, as is the degree of control the service has over placement of the adverts. A Category 1 service may rely on third party intermediaries to display paid advertisements on its service, and so have less control over measures to prevent posting of fraudulent adverts. Both Category 1 and Category 2A services must provide information about any proactive technology they use to comply with their obligations in their terms of service, including when it is used, and how it works. Adverts are fraudulent if they are paid for and breach specified provisions of financial services legislation (for example, carrying on regulated activity under the Financial Services and Markets Act 2000 without authorisation or an exemption). Adverts are paid for if the provider of the service receives consideration (monetary or non-monetary) for them and their placement is determined by systems or processes agreed between the contracting parties involved in the advertisement. This includes “boosted" social media posts where influencers pay to have them promoted more widely. Ofcom is to prepare a code of practice setting out recommended measures to comply with the new obligations.

	Digital Services Act	Online Safety Act
What else do I need to know about the two pieces of legislation?	The DSA covers the infringement of IP rights	The OSA does not include provisions about IP rights
	The DSA imposes transparency requirements in relation to "recommender systems". Users should be able to turn them off.	Draft Ofcom guidance suggests that in-scope services should conduct tests when they update their recommender systems to assess the risk that the changes would increase the dissemination of illegal content.
	The DSA requires service providers to appoint a contact for communication with authorities and a point of contact for users of the services.	The OSA does not include such a requirement (although this may be set out in the Ofcom codes of practice as similar requirements do exist in relation to video sharing platforms (which Ofcom regulates)).
	The DSA includes prohibitions on "dark patterns" (effectively misleading "nudges" such as drip pricing or countdown timers) on online platforms.	The OSA does not include such prohibitions, although the CMA has been active in investigating dark patterns, and there is still scope for them to be included in the Digital Markets, Competition and Consumers Bill as it goes through the parliamentary process.
	The DSA imposes crisis response obligations on VLOPs, if their services have a significant contribution to extraordinary circumstances leading to a serious threat to public security or public health in the EU or a significant part of it.	The OSA does not contain equivalent provisions.
	VLOPs will have to accept the EU Digital Identity Wallet for logging into their online services	Category 1 services must offer all adult users the option of verifying their identity. Adult users may also block anyone who has not verified their identity.
	This is covered in separate legislation, proposed in 2022.	Under the OSA, user-to-user and search services must report child abuse content to the National Crime Agency.
	Providers must respond to orders from judicial and administrative authorities to provide information about specific individual users of their services, but this is a general requirement.	Under the OSA, all providers in scope who publish or place pornographic content on their services must ensure that children are not normally able to see pornographic content, for example, by using age verification procedures.
	Not applicable	The OSA also provides for new criminal offences. These include the false communications offence, aimed at protecting individuals from any communications where the sender intended to cause harm by sending something knowingly false; the threatening communications offence, to capture communications which convey a threat of serious harm, such as grievous bodily harm or rape; flashing offence, aimed at stopping epilepsy trolling; and criminalising assisting or encouraging self-harm online.

LEWIS SILKIN

For more information please contact:

Nick Allan
Partner and Head of Interactive Entertainment

+44 (0)7834 176 677
nick.allan@lewissilkin.com

Geraint Lloyd-Taylor
Partner and Co-Head of Advertising & Marketing

+44 (0)20 7074 8450
geraint.lloyd-taylor@lewissilkin.com