SLAUGHTER AND MAY/

THE EU DIGITAL SERVICES ACT AND UK ONLINE SAFETY ACT: WHERE ARE WE NOW?

FEBRUARY 2025

2025 will see online service providers across the EU and UK continue to grapple with greater regulatory scrutiny, with new obligations either in force or due to apply imminently, all aimed at tackling illegal content and risk on their services.

The Digital Services Act (or '**DSA**'), the EU regulation which imposes far-reaching obligations on providers of online intermediary services, has now been fully in force for over a year. In that time, the Commission has not been shy to exercise its powers, issuing numerous tech companies with requests for information and opening formal investigations into suspected non-compliance.

Meanwhile, in the UK, Ofcom is moving at pace to bring a similar regime – the Online Safety Act ('**OSA**') – into force with effect from 17 March 2025.

In this briefing, we provide a recap of the DSA and explore the Commission's recent enforcement action. We also look at how the OSA compares to the DSA, and outline the steps Ofcom is taking to implement the UK's online safety regime. As we will explain, although the two Acts have similar objectives, the approaches taken by the EU and UK have significant differences – compliance with one will not guarantee compliance with the other.

REMIND ME: WHAT IS THE DSA?

The DSA's main goal, according to the Commission, "*is to prevent illegal and harmful activities online and the spread of disinformation*". It imposes specific obligations on in-scope online service providers, and confirms when such service providers will be exempt from liability for information and content provided by users.

Who does the DSA apply to?

The DSA applies to 'intermediary services', which are divided into three core categories (that align with those already found in the E-Commerce Directive):

- **mere conduits** – services that transmit information, or provide access to a communication network (e.g., internet access providers);
- **caching services** – services that temporarily store user information for efficient onward transmission (e.g., reverse proxies); and
- **hosting services** – services that store user information (e.g., cloud service providers).

The DSA also introduces additional sub-categories of hosting services, which are subject to further obligations:

- **online platforms** – a hosting service that stores and disseminates user information publicly at the user's request (e.g., social media);
- **online marketplaces** – an online platform that allows consumers to conclude distance contracts with traders; and
- **very large online platforms ('VLOPs') and very large online search engines ('VLOSEs')** – online platforms and search engines averaging 45 million+ active users in the EU. The Commission is responsible

for designating platforms and search engines as VLOPs or VLOSEs based on user number information that the DSA requires all online platforms and search engines to publish publicly. To date, the Commission has designated more than 20 platforms as VLOPs (including Facebook, X, Tiktok, Shein and the Amazon Store) and two VLOSEs (Google Search and Bing).

The DSA has extraterritorial effect, capturing intermediary services which have a 'substantial connection' to the EU. This includes not only service providers established in a Member State but also providers outside the EU with a significant number of users in, or which target their activities towards, any Member State(s).

What obligations apply to in-scope services?

The DSA's obligations scale proportionately depending on how services are categorised, and for online platform services and search engines, on their size:

- **VLOPs and VLOSEs** – these services face the most onerous obligations under the DSA, including, crucially, a requirement to assess, mitigate and report any systemic risks stemming from the design, functioning and use made of the service.
- **Other in-scope intermediary services** – smaller players are subject to a shorter list of less onerous obligations (which also apply in any event to VLOPs and VLOSEs). For example, all in-scope services must comply with transparency obligations, including publicly reporting on the content moderation they engage in. Some obligations apply only to hosting services, but not to mere conduits or caching services, e.g., hosting services must introduce mechanisms which enable any individual or entity to notify the service provider of illegal content on the service. Online marketplaces are also subject to additional specific obligations, including an obligation to vet the details of traders using their marketplace.

There is no general obligation on in-scope service providers to monitor the content transmitted or stored on their service, but where a provider does impose content restrictions, that must be done in a diligent, objective and proportionate manner, with due regard to the rights and interests of the parties involved. In assessing and mitigating systemic risks stemming from their services, providers of VLOPs and VLOSEs must also consider how their content moderation systems (along with other factors) influence any such systemic risks.

Summary: DSA Obligations

The below gives a very high-level summary of the obligations introduced by the DSA for caching, mere conduit, hosting and online platform services.

KEY

- Applies to all intermediary services (caching, mere conduits, hosting and online platforms (including VLOPS)) (IS)
- Applies to all hosting services, including online platforms and VLOPs (HS)
- Applies to all online platforms including VLOPs (OP)
- Applies only to VLOPs (VLOPs)

	ISs	HSs	OPs[1]	VLOPs
Cooperate with national authorities following orders to act against illegal content and orders to provide specific information about persons using the service (Art. 9 - 10)	●	●	●	●
Designate a single point of contact for national authorities, the European Commission, the European Board for Digital Services, and for users[2] (Art. 11 - 12)	●	●	●	●
Include information on any restrictions for the use of the service in respect of information provided by users in terms and conditions (Art. 14)	●	●	●	●
Make available reports on any content moderation engaged in at least annually with more stringent requirements for OPs and VLOPs (Art. 15, 24 and 42)	●	●	●	●

[1] There are exceptions for micro or small enterprises.
[2] Where providers of intermediary services do not have an establishment in the EU, but offer services in the EU, they shall also have to designate a legal representative in the EU (Art. 13).

	ISs	HSs	OPs[1]	VLOPs
Introduce mechanisms to allow any entity or individual to notify specific items of information they consider to be illegal content on the platform (Art. 16) and, for OPs and VLOPs, to ensure notices submitted by trusted flaggers are processed expediently (Art. 22) and take action against frequent notices that are manifestly unfounded (Art. 23)		●	●	●
Provide statement of reasons to affected users for restrictions imposed (Art. 17)		●	●	●
Report to the authorities criminal offences detected involving a threat to life or safety (Art. 18)		●	●	●
Provide internal complaint-handling systems and information about available out of court dispute resolution mechanisms (Art. 20 – 21)			●	●
Suspend services to those who frequently provide manifestly illegal content (Art. 23)			●	●
Publish average monthly active EU users every 6 months (Art. 24)			●	●
User-facing transparency so as not to impair the ability of users to make free and informed decisions (Art. 25)			●	●
Online advertising transparency requirements with additional requirements for VLOPs (Art. 26 and 39)			●	●
Bans on targeted adverts to minors (Art. 28) and where the basis of doing so is on sensitive data[3] (Art. 26)			●	●
Transparency of recommender systems in terms and conditions including any options for users to modify those parameters (Art. 27) with users of VLOPs being given the choice to not have recommendations based on profiling (Art. 38)			●	●
Appropriate measures to ensure a high level of privacy, safety, and security of minors on platforms accessible to minors (Art. 28)			●	●
Special obligations for online marketplaces including vetting credentials of traders, compliance by design, random checks on whether illegal content resurfaces, and informing consumers who have purchased an illegal product or service of this fact (Art. 30 – 32)			●	●
Assess, mitigate and report any systemic risks from the design, functioning and use made of the platform's services (Art. 34 – 35)				●
External and independent auditing at own expense and at least annually to assess compliance (Art. 37)				●
Data sharing with authorities and researchers (Art. 40)				●
Establish an internal compliance function (Art. 41)				●
If a crisis occurs leading to a serious threat to public security or health, the Commission may require the provider to take certain actions e.g., to assess whether the services significantly contribute to the threat (Art. 36)				●
Annual supervisory fee (Art. 43)				●

[3] Including data revealing racial / ethnic origin, political opinions, religious / philosophical beliefs and trade union membership, and the processing of genetic / biometric data.

What liability do in-scope services have for user content?

The liability exemptions in the E-Commerce Directive continue to apply. Service providers are not liable for user-provided information, provided they satisfy certain conditions, including that the service provider only plays a passive role in relation to any user-provided information on its service. Significantly, the DSA separates these liability exemptions from the obligations it imposes – a provider's liability (or shield from liability) for user content is not contingent on whether that provider has complied with its DSA obligations.

ENFORCEMENT AND NEXT STEPS FOR THE DSA

What enforcement action is being taken?

While the Digital Services Coordinator ('**DSC**'), an independent authority appointed in each Member State, is responsible for supervising in-scope services in their jurisdiction, the Commission has direct supervision and enforcement powers over VLOPs and VLOSEs.

The Commission has been quick to exercise such powers in the DSA's first year, issuing dozens of requests for information and opening multiple sets of formal proceedings to investigate suspected breaches of the DSA by VLOPs. Some of the most common themes from such investigations are suspected breaches of the following obligations (the first three of which apply to VLOPs and VLOSEs only, and latter two of which apply to all hosting platforms):

- to assess and mitigate systemic risks stemming from the design or functioning of a service (Articles 34 and 35);
- to provide a publicly available repository of details about online advertisements (Article 39);
- to provide researchers with access to public data (Article 40(12));
- to provide 'notice and action' mechanisms (Article 16); and
- to ensure a high level of privacy, safety and security of minors (Article 28(1)).

Other DSA obligations cited in the investigations include those relating to the prohibition on deceptive and manipulative design of online interfaces, and requirements for any system used to recommend content to users to be transparent.

Enforcement action to date indicates that the Commission intends to take a very robust approach to regulating the most powerful and widely used platforms. That such wide-ranging and comprehensive investigations have been conducted in such a short period is of note, with each relevant VLOP being investigated for multiple suspected breaches. In the case of AliExpress, the Commission is examining potential breaches of ten separate DSA articles.

There are also signs that enforcement action is having an impact, with TikTok and LinkedIn both disabling functionality in the EU as a result of Commission interest.

Notably, the breaches being investigated by the Commission do not relate solely to DSA obligations which are applicable to VLOPs and VLOSEs only. They include breaches of standard obligations applicable to all hosting platforms that could also have been investigated by the relevant DSC. We expect the Commissions' findings will set the standard for how the relevant obligations will be imposed going forward in all Member States.

Preliminary findings against X

To date, the Commission has only announced preliminary findings in respect of one investigation. On 12 July 2024, it published its preliminary view that the 'verified accounts' aspect of X's interface is deceptive, that X fails to provide a compliant repository of advertisements, and that X does not permit researchers independent access to its public data. X was entitled to examine the Commission's investigation file, and respond to the findings, prior to any final decision being made, although X owner Elon Musk has said he "*look[s] forward to a very public battle in court*".

The Commission's investigation into X, and enforcement of the DSA generally, has drawn US political attention and criticism in the context of the 2024 US presidential elections. In particular, J.D. Vance, the then-incoming US vice president, seemed to suggest that the US should consider pulling its support of NATO if the Commission took action against X for breaches of the DSA (on the grounds that Vance viewed this as not respecting American values and free speech). The headlines this has generated have included speculation that pressure from the US, coupled with pressure to improve economic growth in the EU, might dissuade the Commission from pursuing American technology companies like X.[4]

However, on 17 January 2025, the Commission indicated that the investigation was continuing by taking three further steps:

[4] *Will Europe ease up on big tech?*

- requesting X to provide its internal documentation on the platform's recommender systems (e.g., the algorithms used to recommend content to users);
- issuing a retention order requiring X to preserve internal documents and information regarding future changes to the design and functioning of its recommender systems; and
- issuing a request for access to certain of X's APIs.

The Commission said that these steps will allow it to "*take all relevant facts into account in the complex assessment under the DSA of systemic risks and their mitigation*".

What are the consequences of non-compliance?

Under the DSA, the maximum fines are:

- for non-compliance – up to **6% of the infringer's annual global turnover**; and
- for knowingly or negligently submitting incorrect, incomplete or misleading information – up to **1% of the infringer's annual global turnover**.

DSCs and the Commission also have powers to require service providers to take immediate actions where necessary to address very serious harms. In extreme scenarios, the DSA envisages that a service may be restricted in a Member State if an infringement causing serious harm is not remedied.

In the case of X, the Commission has already announced that if its findings are confirmed, it "*will impose fines and require significant changes.*"

What's coming next?

Standards and best practice for future compliance, and any enforcement for suspected non-compliance, will continue to evolve as DSCs publish guidelines (see, for example, those published by the Dutch DSC) and start to take their own enforcement action, and as new implementing regulations are published by the Commission.

Draft guidelines on compliance with Article 28 of the DSA (regarding the protection of minors on online platforms) are also expected to be published early this year. From July to September 2024, the Commission ran a call for evidence on those guidelines to gather input from stakeholders on their scope, approach and content. For thousands of platform providers, these guidelines will constitute the most consequential guidance published by the Commission in these early years of the DSA. As stated in the call for evidence, the guidelines will "*apply to all online platforms, including those that are aimed at adults… but that still have underage users due to inadequate or non-existent age-verification tools.*" Themes that can be expected to feature are age verification, systems for recommending content to minors, and addictive design of online platforms.

REMIND ME: WHAT IS THE OSA?

The OSA is a new set of laws aimed at making the UK "*the safest place in the world to be online*". The legislation received parliamentary approval in autumn 2023, but is being brought into force gradually by Ofcom, the regulator appointed to oversee its implementation and enforcement.

In-scope services. Two main types of service are caught under the OSA: 'user-to-user services' and 'search services'.

- **User-to-user services.** While headlines tend to focus on the OSA 'taming' large social media sites, the concept of 'user-to-user services' is very broad, capturing any internet service which allows at least one user to encounter content shared by another. It is defined as an 'internet service by means of which content that is generated directly on the service by a user of the service, or uploaded to or shared on the service by a user of the service, may be encountered by another user, or other users, of the service'.

  The fact that any such 'user-to-user service' may be only a minor or ancillary part of a company's activities, or that such service may only have a small number of users, would not take it out of scope of the OSA requirements. For example, an online help forum with a small number of users would still be subject to a considerable compliance burden under the OSA. There have already been reports of specialist forums (including one with 50,000 members) choosing to close down due to a lack of resources to support OSA compliance.[5]
- **Search services.** Search services are internet services that include a search engine, and search engines are services or functionalities that enable users to search more than one website or database.

[5] *Online Safety Act's obligations spark concern among small site owners*

As such, this category does not merely capture household names such as Google or Bing. Ofcom has also confirmed that it encompasses 'vertical' search engines, which can include comparison websites where users search and compare particular products.

Notably, generative AI models, which would not traditionally be viewed as 'search engines', are in scope if they operate by searching multiple sites or databases. Ofcom published an open letter on 8 November 2024 following a number of concerning cases of use of GenAI chatbots, including one in which such a chatbot was created to act as a virtual clone of deceased children.[6] That open letter emphasised that the OSA applies to certain GenAI chatbots and search tools, as well as to AI-generated content which is shared with other users.

- **UK nexus.** Similar to the position under the DSA, which regulates entities with a 'substantial connection' to the EU, the OSA only regulates both types of services if they have 'links with the UK'. Importantly, this does not require that the service have a high number of UK users. If the UK is a target market for the service, or there is good reason to believe that UK users may suffer significant harm on the platform, the OSA will likely apply.
- Ofcom tool. Ofcom have published a user-friendly tool to help providers understand if their service is likely to be in-scope.

OSA obligations. The OSA imposes a wide range of general obligations, including:

- **Illegal content risk assessment.** Providers must conduct a 'suitable' and 'sufficient' assessment that assesses the risk of users encountering illegal content on a service, and the risk and severity of harm they may face from such content. User-to-user services will also need to assess the risk of their service being used to commit criminal offences. This must be kept up-to-date, and a further assessment is required each time a service makes any 'significant change' to its design or operation.
- **Safety duties concerning illegal content.** Providers must use proportionate measures, processes and systems to prevent users on 'user-to-user services' encountering particular categories of 'priority' illegal content (such as child abuse content), and swiftly take down any illegal content once on notice. For search services, they must minimise the risk of individuals encountering illegal content. For both types of service, providers should effectively mitigate the risks of harm to individuals.
- **Content reporting and complaints.** Users must be able to report illegal content easily, and providers must operate complaints procedures that are easy to access, easy to use, transparent, and which provide for appropriate action to be taken. Users should be able to complain about, among other things, the removal or de-prioritisation of their content and actions taken against them, as well as a provider's non-compliance.

There are also additional duties for those services 'likely to be accessed by children'.

Ofcom Codes. In-scope providers are expected to satisfy the applicable requirements of the OSA by adopting specific measures which are set out in detailed Codes of Practice which have been, or will be, issued by Ofcom. As we note below, Ofcom's first Codes of Practice, which deal with the duties in the OSA relating to illegal content, have now been published. These Codes contain 41 specific measures for user-to-user services and 33 for search services, and cover, among other things:

- governance and accountability requirements (such as nominating an individual accountable for online safety, and conducting compliance training);
- content moderation requirements (including a requirement for certain services to adopt specific technologies, such as 'hash matching', and to have a policy on how content is prioritised for review);
- reporting and complaints requirements (such as providing indicative timelines for complaint handling);
- a requirement that certain services collect safety metrics when testing algorithm changes; and
- user controls and default settings.

In-scope services will need to work through the proposed measures carefully to determine which apply - whether a particular measure applies to a service can depend on its size, its risk profile, and/or whether it is particularly exposed to a specific type of harm or contains certain functionality (e.g., file storage or a recommender system).

Enforcement. If a provider is found not to have complied with their OSA duties, Ofcom's enforcement powers include the ability to issue substantial fines – up to the greater of £18 million or 10% of global annual revenue.

[6] *Digital clones of Brianna Ghey and Molly Russell created by 'manipulative and dangerous' AI*

NEXT STEPS AND PREPARING FOR COMPLIANCE

Ofcom is implementing the OSA in three phases. Below is a summary of the key aspects of each phase, along with important deadlines that are approaching that providers should be keeping in mind.

Phase one: illegal harms

This first phase will see the 'illegal content safety duties' enter into force. These constitute the base level duties to mitigate and manage the risk of harm to users arising from exposure to illegal content and activity which regulated user-to-user services and search services must comply with.

16 MARCH 2025

Illegal content risk assessment. In-scope user-to-user and search services must assess the risk of illegal content being present on, and, for the former category, criminal offences being committed via, their services, by no later than 16 March 2025.

Ofcom has published guidance on the four-stage approach it expects providers to take. Providers must, as a minimum, individually assess the risk level of a service by reference to 17 types of 'priority illegal content'. It will not be possible to properly determine which measures in Ofcom's 'Illegal Content' Codes of Practice apply to a service until the assessment is completed.

17 MARCH 2025

'Illegal Content' duties enter force. Ofcom published its 'Illegal Content' Codes of Practice on 16 December 2024. The size, and risk profile of a service (determined by completing the required risk assessment), will determine which measures apply.

Provided such Codes clear the UK parliamentary process, Ofcom will be able to enforce against services that are failing to comply with the applicable measures in the Codes, or that have failed to adopt alternative measures which ensure OSA compliance, from 17 March 2025.

Phase two: child safety

The second phase primarily concerns providers assessing if they are 'likely to be accessed by children', and if so, the measures that need to be implemented as a result.

16 APRIL 2025

Children's access assessments. In-scope user-to-user and search services must assess whether children are likely to access their services and in what numbers. Providers can only conclude that children cannot access a service if they deploy age assurance techniques which are 'highly effective' in blocking children accessing their service. If a significant number of children use a service, or the service is likely to attract significant numbers of child users, additional duties will apply to protect those users from certain 'harmful' content. In-scope providers must conduct their children's access assessment by 16 April 2025.

APRIL 2025

Ofcom guidance on children's risk assessment and codes. Ofcom will publish its guidance for conducting children's risk assessments, and 'Protection of Children' Codes of Practice, in April 2025.

JULY 2025

Children's risk assessment. Relevant services should complete this assessment by no later than the end of July 2025. This assessment focuses on the risks to children from encountering harmful content. It is additional to the illegal content risk assessment, and must be conducted if the children's access assessment concludes that the service is 'likely to be accessed by children'.

Child safety duties enter force. The 'Protection of Children' Codes of Practice will enter force in July 2025. Relevant services must ensure the child safety duties in the OSA are complied with (either by adopting the applicable measures in the Codes or by otherwise satisfying the OSA's requirements as to the protection of children).

Phase three: categorised services

The final phase deals with the additional duties that will apply to the small number of 'categorised' services, being those which are so designated by Ofcom on the basis of size and/or the risk posed by the service.

SUMMER 2025	Ofcom is to publish its initial register of categorised services.
AUGUST – NOVEMBER 2025	Ofcom is to issue transparency notices to categorised services. Categorised services will have to publish transparency reports annually containing information relating to their service which Ofcom has required be included in a transparency notice.
EARLY 2026	Ofcom is to publish Codes of Practice regarding the additional duties that apply to categorised services by no later than early 2026.

Ofcom has also published a range of additional guidance relating to the OSA, which providers should consult. This includes guidance on:

- how providers should determine if they have age assurance methods that are viewed by Ofcom as being 'highly effective';
- how providers should decide whether content is 'illegal' for the purposes of the Act;
- what providers must do in terms of keeping records of compliance; and
- how to determine whether content is 'publicly' or 'privately' communicated (as some measures in Ofcom's Codes of Practice will not apply to 'private' communications).

HOW DOES THE OSA DIFFER FROM THE DSA?

The OSA, as with the DSA, seeks to regulate online services, with a key aim of tackling illegal content and making the internet a safer place. There is a degree of overlap between the OSA and DSA in the types of obligations each imposes.

However, while there are similarities, each Act takes a different approach. Generally, the DSA is broad and covers a comprehensive scope of issues, but at a higher level. The OSA, by comparison, is a considerably longer piece of legislation that is more granular in terms of the specificity of the obligations imposes, and is more focussed than the DSA on requiring providers to take proactive steps to moderate illegal content and certain harmful content.

Each Act also has its own set of distinct concepts and obligations that do not neatly reconcile. As such, compliance with the DSA will not necessarily ensure compliance with the OSA, and there is no 'one-size-fits-all' approach to ensuring both regimes are met. In-scope services which fall under both regimes will need to determine what the OSA requires of them, and whether their existing practices – which may have been implemented to comply with the DSA – are sufficient.

KEY SIMILARITIES	KEY DIFFERENCES
Regulation of online services • Both the OSA and DSA generally target online services. Social media, online marketplaces, video-sharing platforms, dating apps, online forums, and messaging services are examples of the types of services that are within the scope of both Acts. **Overlapping obligations** • There is a degree of overlap in the OSA and DSA's obligations, with both addressing: - services having in place a process for users to flag content; - services having effective complaint-handling systems; - what needs to be covered in terms of service; - services undergoing risk assessments; and - having an internal compliance function dedicated to online safety matters. **Extra-territorial effect** • The OSA and DSA both have extra-territorial effect. The OSA applies to in-scope services that have 'links with the UK', and the DSA applies to in-scope services with a 'substantial connection' to the EU (albeit the specific tests applied to determine if the relevant nexus is present differ slightly between the Acts).	**Categories of in-scope services** • The test applied under the DSA to assess whether a service is 'in scope' is broader than under the OSA. The OSA and DSA also categorise services differently, using concepts that do not align: - The OSA's concept of 'user to user services' overlaps with but is not exactly equivalent to the DSA's concepts of 'hosting services' or 'online platforms'. The OSA also has no equivalent for the DSA's categories of 'mere conduit' or 'caching' services, which capture a broader range of intermediary services than are covered by the OSA. - The concept of 'search services' in the OSA is broader, given it captures any functionality that searches more than one website or database (which can include vertical search engines and GenAI tools). By contrast, the DSA's corresponding concept – 'online search engines' – only captures sites where users can, in principle, search all websites. Debate as to how this DSA definition applies to GenAI tools has arisen in recent months, given that some GenAI tools do incorporate website results and others do not.[7] However, even if not captured as search engines, the DSA could still apply to vertical search engines and GenAI tools where they qualify as intermediary services (e.g., as hosting services, on the basis that they store information provided by users). - The OSA specifically regulates access to pornographic sites / content, whereas the DSA does not contain specific provisions on this (although, again, where such services qualify as intermediary services, they will be nevertheless be regulated by the DSA in the same way as any other intermediary service, and a number of online platforms that host and disseminate pornographic content have been designated as VLOPs under the DSA).

[5] *From ChatGPT to Google's Gemini: when would genAI products fall within the scope of the DSA?* | Media@LSE

KEY SIMILARITIES

Protection of minors

- The OSA and DSA both specifically address the protection of children online. The OSA will require in-scope services that are 'likely to be accessed by children' to comply with specific measures set out in 'Protection of Children' Codes of Practice published by Ofcom. The DSA contains a general obligation to ensure a 'high level of privacy, safety, and security' for minors, with further detailed guidance expected from the Commission this year.

Scaling of obligations

- The OSA and DSA both have a tiered approach. The OSA will apply additional obligations to 'Category 1' and 'Category 2B' services (capturing the largest / riskiest social media sites) and 'Category 2A' services (capturing the largest / riskiest search services). Similarly, the DSA places the greatest compliance burden on VLOPs and VLOSEs, i.e., those online platforms and search engines averaging 45 million or more monthly users in the EU.

Significant fines

- Both the Commission and Ofcom can impose substantial fines for non-compliance with the DSA or OSA (respectively). For the DSA, fines can be issued for up to 6% of the infringer's annual global turnover, and for the OSA, up to the greater of £18 million or 10% of global annual revenue.

KEY DIFFERENCES

Differences in specific obligations imposed

- Some obligations imposed by the DSA have no parallel in the OSA, and vice versa. For example, the following provisions of the DSA do not have equivalents in the OSA:
  - Providers of online platforms must not use dark patterns (i.e., must not design, organise or operate their online interfaces in a way that deceives or manipulates users).
  - Service providers have obligations relating to the 'traceability' of online traders using online marketplaces, and have transparency obligations for online advertisements on their services.
  - VLOPs and VLOSEs must provide vetted researchers with access to data for the purpose of research into systemic risks in the EU.
- Also, as noted above, under the DSA, there is no general obligation on providers to monitor user activity, but they must report on the content moderation they do engage in (and only providers of VLOPs and VLOSEs must consider how their content moderation systems influence any systemic risks stemming from their services). By contrast, the OSA essentially assumes that all providers will have a content moderation function that can swiftly take down illegal content.

Regulated content

- The DSA applies to illegal content (which will necessarily differ across Member States). The OSA applies to illegal content (subject to a small number of specific exclusions, such as IP infringement), but also specifically regulates 'content that is harmful to children', as defined in the Act.

Risk assessments

- While both Acts envisage services risk-assessing their platforms and putting mitigations in place, this only applies to VLOPs and VLOSEs under the DSA. The OSA requires all providers, regardless of size and resource, to conduct a thorough risk assessment of their services.

Exemptions for small businesses

- The DSA excludes businesses that qualify as small or micro enterprises from the obligations applicable to online platforms (although not to the general obligations applicable to all intermediary services). The OSA does not contain any specific exemptions for small businesses, but the legislation is drafted to recognise that what is 'proportionate' depends on the size and capacity of the provider, and this is also baked into the Codes of Practice.

OUR DIGITAL REGULATION PRACTICE

As digital adoption increases, and governments and regulators across the globe grapple with how best to regulate new advancements, you need to ensure that you have considered and managed a wide range of issues when developing or deploying new digital solutions. Technological developments create new opportunities and risks, and regulators and legislators are considering how new laws and guidance will fit into the existing matrix of regulation.

We are helping our clients navigate this changing landscape. We regularly publish insights on Digital Regulation and share developments on our digital blog, The Lens.

OUR TEAM

ROB SUMROY
Partner – London
+44 (0)20 7090 4032
rob.sumroy@slaughterandmay.com

ALEXANDER CHADD
Partner – Brussels
+32(0)2 737 9419
alexander.chadd@slaughterandmay.com

NATALIE DONOVAN
Head of Technology, Digital, Data and IP Knowledge – London
+44 (0)20 7090 4058
natalie.donovan@slaughterandmay.com

CATHERINE O'CALLAGHAN
Associate – London
+44 (0)20 7090 3552
catherine.ocallaghan@slaughterandmay.com

JACK HIGGINS
Associate – London
+44 (0)20 7090 5111
jack.higgins@slaughterandmay.com

LUIS GUINCHO
Associate – Brussels
+32(0)2 737 9456
luis.guincho@slaughterandmay.com