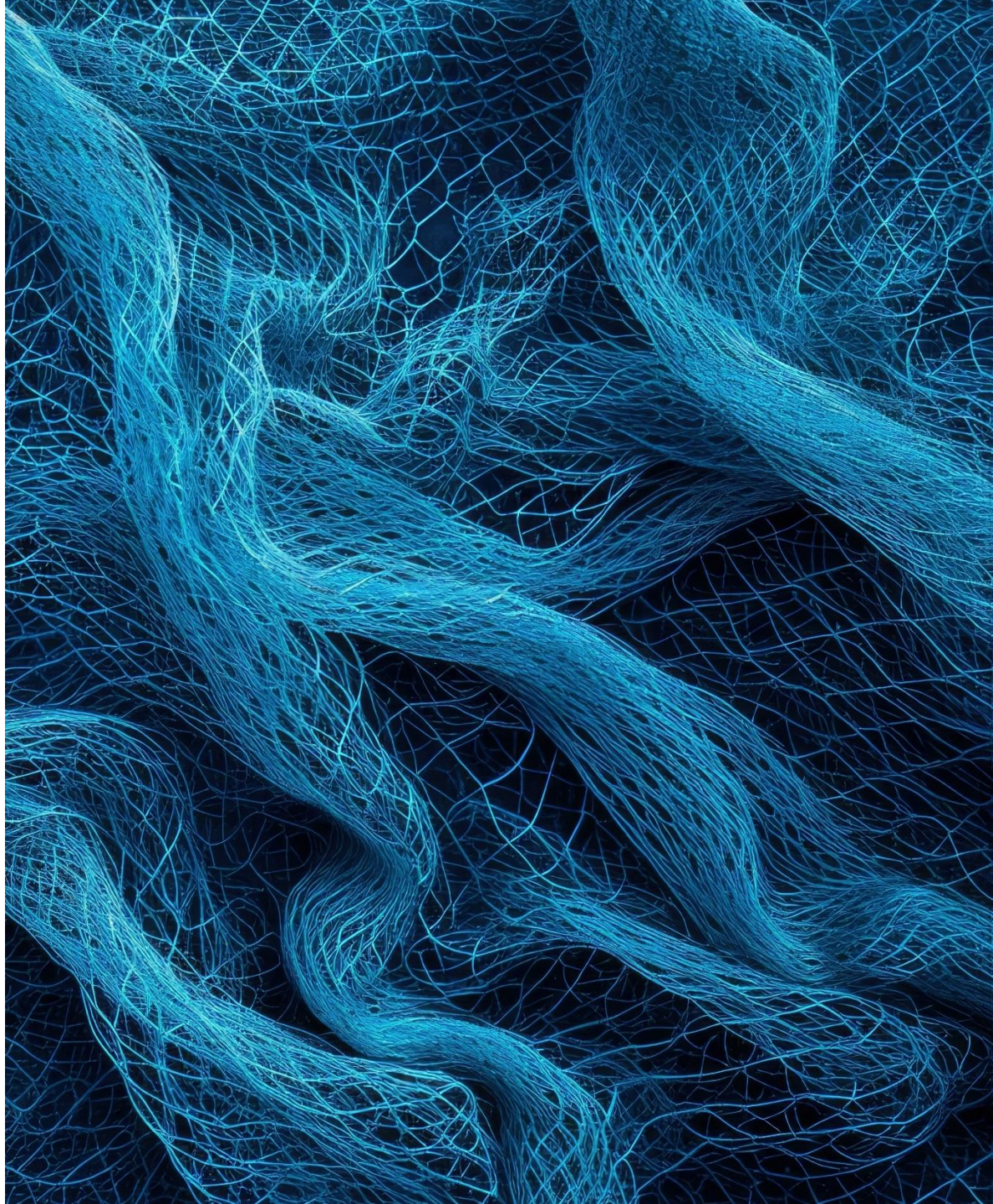
Bristows

OSA vs DSA

Comparing the UK and EU online safety regimes

The UK Online Safety Act (**OSA**) and the EU Digital Services Act (**DSA**) share a common goal of creating safer online spaces, but they feature their own distinct approaches and nuances. While the OSA focuses heavily on protecting users, especially children, from illegal or harmful content, the DSA emphasises transparency, accountability, and systemic risk management. Our table below explores how these two frameworks align, where they diverge, and what their impact means for digital services.



Click to navigate

- Introduction
- Timeline
- Scope
- Territory
- Cumulative scale of obligations
- Key obligations
- Content moderation
- Transparency / terms of service
- Recommender systems and advertising transparency
- Protection of children, and women and girls
- Risk assessments
- Guidance and codes of practice
- Enforcement

OSA	DSA
Introduction	
The OSA is the UK's legislative framework for a new regulatory regime aimed at making the internet safer for UK users. It seeks to do this by changing and increasing the liability of in-scope online service providers to require them to take a proactive approach to managing the safety risks encountered by users. This extends to in-scope service providers that operate outside the UK. The first set of duties on in-scope service providers became enforceable in December 2024; the remaining duties will become enforceable in phases through to 2027. The framework provided by the OSA will be supported through codes of practice and guidance issued by Ofcom and through secondary legislation. These will collectively form one of the most far-reaching and comprehensive online safety initiatives in existence globally. The OSA applies to three main types of online service: (i) user-to-user (U2U), (ii) search engines; and (iii) pornography services, as described further in the *Scope* row below.	The European Commission's main goal for the DSA is to create a safer digital space in which the fundamental rights of all users of digital services are protected. It therefore shares a common aim with the OSA of making the internet a safer place. However, the DSA has been prepared to complement and add to the fast-growing library of EU regulations, and so interacts heavily with existing concepts and nuances that are well established in EU law. Most obviously, the DSA was released in tandem with the competition law-focused Digital Markets Act (DMA), providing a "package" of new rules to regulate different aspects of online services. As the GDPR did in the data protection space, the DSA builds on key protections for EU citizens enshrined in the Charter of Fundamental Rights of the European Rights of the European Union, and applies a graduated set of rules to different types of "intermediary services" using concepts from the EU's previous 2000 eCommerce Directive (discussed further in the *Scope* row below).
Timeline	
The timeline for the application of the OSA's provisions is more complicated than the DSA equivalent. It received Royal Assent on 26 October 2023, with compliance deadlines for different portions of the Act being dictated by the publication of the final version of the relevant Ofcom codes of practice and guidance documents (and completion of the associated parliamentary process). For example, Ofcom's powers to enforce the OSA's illegal harms obligations (under its phase 1) began on 16 March 2025, falling 3 months after it published its Statement and finalised codes of practice and guidance on illegal harms. See further our Implementation timeline article for a summary of key OSA dates, and Ofcom's Important dates for Online Safety compliance.	For the DSA, the enforcement timeframe is more straightforward. Most of the DSA's provisions have applied since 17 February 2024. Additional obligations apply to very large online platforms / search engines (**VLOPs** / **VLOSEs**) from 4 months after their designation as such by the European Commission. These types of services, the designation process and the additional obligations that apply to them are described further below.

OSA	DSA
Scope	
The OSA applies to three main types of online service: (i) user-to-user, (ii) search engines; and (iii) pornography services. The safety measures that the Act requires service providers to implement will vary depending on the size of the service and how "risky" the service is perceived to be. Consequently, the preparation of multiple risk assessments is a major focus of the OSA, for which Ofcom consultations, codes and guidance continue to develop. In practice, this means that the OSA applies to a wide range of online services, including social media and messaging platforms, video sharing platforms, search engines and comparison sites, and other websites that host user-generated content, such as file sharing and storing sites and user forums and chatrooms. Ofcom has estimated that over 100,000 service providers may be in scope. The OSA places additional duties on (i) services likely to be accessed by children, and (ii) services that meet certain thresholds set out in secondary legislation so that they constitute a "**Category 1**", "**Category 2A**" or "**Category 2B**" service. These categories are described further in the *Cumulative scale of obligations* row below. The scope of services caught by the OSA is comparatively broader than those in scope of the DSA. For example, more rules will apply to direct messaging services (which are expressly in scope of the OSA), and potentially to more fast-developing generative AI services (such as LLM-powered chatbots) on a wider range of platforms. A service will also need to have a 'UK link' in order to be subject to the OSA (described further in the *Territory* row below). See further this section of The Safety Net for a more detailed explanation of the scope of the Online Safety Act.	The DSA takes a different approach, building on service definitions that are already established in EU law. It applies to "information society services" which are "intermediary services". It further sub-categorises intermediary services into: • **mere conduit services**, e.g., internet exchange points, wireless access points, VPNs, DNS services • **caching services**, e.g., content delivery networks, reverse proxies, content adaptation proxies • **hosting services**, e.g., cloud computing, web hosting, file sharing, online platforms These sub-categories are then split into online platforms or search engines: • **online platforms** (a type of hosting service), e.g., social networks, online marketplaces • **online search engines**, e.g., web search providers Finally, online platforms or search engines will be categorised as very large online platforms / search engines (**VLOPs** / **VLOSEs**) if they have at least 45 million average monthly active users/recipients within the EU and are designated as such by the European Commission. The DSA's requirements increase cumulatively, so that intermediary services that are not hosting services (or VLOSEs) have the fewest DSA obligations, while VLOPs and VLOSEs have the most obligations. For example, in contrast to the OSA, direct messaging services might fall under the DSA's "mere conduit" category and face significantly fewer obligations. There are also question marks over how the DSA will apply to various generative AI services such as chatbots, which do not fit neatly into any one DSA service category. By contrast, the OSA's broad service definitions (discussed adjacent) provide the Act with a more straightforward means to apply to a range of generative AI-powered services; a point which Ofcom emphasised in its open letter to online service providers in November 2024.

OSA	DSA
Territory	
A service will be regulated by the OSA if it has “links to the UK” and is not exempt. The UK links test is met if a service has (i) a “significant number of UK users”, (ii) the UK forms part of the service’s “target” market, or (iii) the service is capable of being used in the UK and there are reasonable grounds to believe that the content on the service presents a “material risk of significant harm” to UK users. Element (iii) is novel since it could potentially catch services provided outside the UK to users who are also outside the UK. This is quite an ambitious reach, and it is yet to be seen how Ofcom may seek to apply this type of extra-territorial scope in practice.	An intermediary service will be regulated by the DSA where it has a "substantial connection" to the EU. This may arise from the provider’s establishment in the EU or from factual criteria such as the targeting of activities towards one or more Member States (criteria which will be familiar to GDPR professionals), or the service having a “significant number” of recipients in one or more EU Member States.
Cumulative scale of obligations	
The OSA applies a significant core of its obligations to both U2U and search services. It then places additional duties on (i) services likely to be accessed by children, and (ii) services that meet certain thresholds set out in secondary legislation so that they constitute a **Category 1**, **Category 2A** or **Category 2B** service. The relevant thresholds as follows: • **Category 1** should apply to services that either: (i) use a recommender system and have more than 34 million UK users on the U2U part of the service (around 50% of the UK population), or (ii) allow users to reshare user-generated content, use a content recommender system and have more than 7 million UK users on the U2U part of the service (around 10% of the UK population). • **Category 2A** should apply to horizontal search services with more than 7 million UK users. • **Category 2B** should apply to services which allow users to send direct messages and have more than 3 million UK users on the U2U part of the services. Categorisations of services based on this criteria will be carried out and published by Ofcom. This process is similar to the categorisation of VLOPs and VLOSEs by the European Commission under the DSA, except that Ofcom’s categorisation factors in more service functionality nuances in addition to looking at UK user numbers.	The DSA also cumulatively scales up obligations depending on the relevant type of service. For the DSA, this is based on its definitions which build on existing EU concepts. In order of increasing applicability of obligations, these are: • mere conduit or caching services (least obligations) • hosting services • online platforms (a type of hosting service) • online consumer marketplaces (a type of online platform) • VLOPs and VLOSEs (most obligations) As mentioned in the *Scope* row above, online platforms or search engines will be categorised as VLOPs or VLOSEs where they have at least 45 million average monthly active users/recipients within the EU and are designated as such by the European Commission. The European Commission has so far designated 17 VLOPs and 2 VLOSEs according to this criteria. The full list is published by the Commission here. The DSA does not have an equivalent set of specific obligations for pornography service providers as is the case for the OSA.

OSA	DSA

Key obligations

The OSA's core obligations that apply to in-scope service providers under the first two headings (*illegal harms and protection of children*) are wide-ranging and broadly cover:

- Carrying out risk assessments
- Implementing measures to safeguard users and, in particular, to protect child users, e.g., in relation to content moderation
- User empowerment, including duties relating to user settings and having an appropriate user complaints process
- Safety measures around the design of a service
- Specific requirements relating to a provider's terms of service
- Governance and accountability

Additional or enhanced obligations apply to **Category 1**, **2A** and **2B** services. Depending on which of these categories a service falls into, these obligations relate to key aspects including:

- Transparency reporting
- Risk assessments and recording keeping
- Protections for news and journalistic content
- Identity verification options
- Preventing fraudulent advertising

The OSA's obligations on providers of pornography services are narrower and primarily cover implementing effective age assurance measures to ensure that minors cannot access the service, and related record-keeping duties.

The DSA's core obligations apply to online platforms under the following key themes:

- **Illegal content**: hosing services (including online platforms) must implement notice and action mechanisms for users, and "trusted flaggers", to report content to the provider to process and decide on in a timely and diligent manner
- **Manipulative tactics**: the DSA prohibits deceptive design patterns in online interfaces that can impair users' decision-making
- **Content recommender systems**: platforms must provide transparency information about how their recommender systems work, and about any options for service recipients to adjust them
- **Freedom of expression**: platforms must implement an appropriate user complaints process, allowing users to challenge content moderation decisions
- **Advertising**: platforms must ensure certain transparency information about adverts is shown to users. Targeting ads to children based on personal data profiling is prohibited, and targeting ads to anyone based on special category data profiling is prohibited

Additional obligations apply to VLOPs and VLOSEs, including:

- Carrying out assessments in relation to systemic risks
- Mitigating systemic risks
- Additional transparency requirements for terms and conditions
- Additional audit and transparency reporting requirements
- Establishing a point of contact for users and authorities

We provide a breakdown of similarities and differences between some of these key OSA and DSA obligations below.

OSA	DSA
Content moderation	
Compared to the DSA, the OSA requires regulated service providers to take a more proactive approach to regulating harmful content on their platforms, and has rules applying to both illegal content and content which is not illegal but which is harmful to children in the UK, or which presents a material risk of significant harm to children in the UK. Under the OSA, “illegal content” is that which “amounts to a relevant offence”. In its guidance, Ofcom lists “priority” and “non-priority” offences which would *all* constitute illegal content, but which carry with them different content moderation duties. **For illegal content**: Both search and U2U service providers should implement general content moderation measures to swiftly remove, index, and re-rank illegal content. Further, larger providers of medium and high risk services will be required to make use of automated tools to make content moderation processes more effective and efficient. Ofcom expects that using such tools may require a tailored approach depending on the organisation and the type of content at issue. **For content that is harmful to children**: U2U and search services should restrict content that is harmful to children through effective moderation. This moderation can be done automatically, by way of human moderation or through a combination of the two. Large search services should deploy a ‘safe search’ setting where, if a user is believed to be a child, Primary Priority Content in particular should be identified, downranked, and if necessary, blurred out. For further detail see our Illegal harms article.	The DSA defines “illegal content” as any information that is itself illegal or relates to an illegal activity under EU or Member State laws. Unlike the OSA, the DSA does not require proactive content moderation. The liability exemptions contained in the 2000 eCommerce Directive which exempt information society service providers from liability for illegal information for which they are a "mere conduit", or which they just cache or host, have been carried forward into the DSA. However, under the DSA, for hosting services to benefit from the liability exemption, the provider needs to implement “notice and action” mechanisms for illegal content, in response to both orders from Member State authorities and user reports. When providers respond to user reports, the DSA requires providers to explain their decisions and how they can be challenged. In contrast to the OSA, the DSA does not place specific obligations on providers for content which is potentially harmful but not illegal. However, the risk assessment and mitigation obligations placed on VLOPs and VLOSEs (discussed further in the *Risk assessments* row below) are likely to apply to illegal or otherwise harmful content that pose systemic risks to users relating to the functionality of the platform.

OSA	DSA

Transparency / terms of service

The OSA contains several requirements in relation to what regulated service providers must include in their terms of service. These include:

- specifying how individuals are to be protected from illegal content, users' rights to bring claims, and complaints handling policies
- giving information about any proactive technology used by a service to comply with the provider's safety duties under the Act
- **for services likely to be accessed by children**: how children are protected from different types of content regulated by the OSA
- **for Category 1 services**: summarising the findings of the service's most recent illegal content risk assessment
- **for Category 1 services likely to be accessed by children**: summarising the findings of the service's most recent children's risk assessment
- **for Category 1 and 2 services**: specifying what their policy is about dealing with requests from parents of a deceased child for information about the child's use of the service

The OSA requires that terms of service are clear, accessible and consistently applied.

All intermediary services must set out, in their terms and conditions, information about any restrictions that they impose regarding the use of their service in respect of user content. This includes information on any policies, procedures, measures and tools used for the purpose of content moderation, including algorithmic decision-making and human review, as well as the rules of procedure of their internal complaints handling system. VLOPs and VLOSEs must also publish annual reports setting out the results of their DSA risk assessments (as described further in the *Risk assessments* row below).

As can be seen, while the requirements are structured and written differently in the OSA compared to the DSA, their themes are similar. Both Acts aim to increase transparency in regulated providers' terms of service regarding key aspects relating to online safety: what rules apply to content and activity on the service, what systems, processes and tools (with the OSA focusing especially on "proactive technology") are in place to promote safety on the service, and what their complaints handling procedures and policies are. Both Acts also require certain types of larger / higher risk services to publish summaries of their risk assessments carried out under the relevant Act.

Recommender systems and advertising transparency

Both the OSA and the DSA contain requirements about regulated services' recommender systems; that is, how the services' algorithms select what kinds of content to show or promote to users. This reflects increasing regulator concerns about the proliferation of illegal or harmful content across online services, including worries about children or other vulnerable types of users falling into so-called "doom loops" when consuming content (where negative types of content become increasingly prominent the more a user interacts with them).

For VLOPs and VLOSEs specifically, the DSA expressly requires such services to take into account the design of their recommender systems and any other relevant algorithmic system as part of their DSA risk assessments. This aspect of the DSA is not as focused on harms to children as the equivalent in the OSA, although the DSA does require such risk assessments to consider, amongst other things, any particular risks to the rights of children.

(Continued on next page)

OSA	DSA
Recommender systems and advertising transparency (cont.)	
Ofcom guidance places a focus on the importance of safer algorithms for child users, for example recommending that services that use recommender systems should configure their algorithms to filter out the most harmful content. Ofcom also suggests that U2U services operating recommender systems *should not* recommend any Primary Priority Content to children and that Priority Content should be reduced in prominence. The OSA does not contain specific provisions about recommender system transparency or advertising transparency that are equivalent to those contained in the DSA (described adjacent). Instead, it places certain obligations on **Category 1** and **Category 2A** services to tackle fraudulent advertising. The UK Government also launched an Online Advertising Programme to review the regulatory framework of paid-for online advertising, to tackle illegal and legal but harmful advertising, as well as the lack of transparency and accountability across digital advertising supply chains. This Programme is intended to work alongside the OSA.	The DSA contains more specific transparency provisions about recommender systems and advertising transparency compared to the OSA. It requires that all online platforms that use recommender systems explain in their terms and conditions the main parameters used in their recommender systems, as well as any options for the recipients of the service to modify or influence those main parameters. For all online platforms, the DSA contains specific requirements about transparency information that must be provided for adverts on online interfaces. This information must enable recipients to identify in real time: (i) the fact that the information is an advert, (ii) on whose behalf the advert is shown, (iii) the person who paid for the advert, and (iv) meaningful information about the main parameters used to determine the recipient to whom the advert is presented and how to change those parameters. The DSA also prohibits: (i) targeting adverts to children based on the profiling of their personal data, and (ii) targeted adverts to anyone based on the profiling of special category data (as defined in the GDPR).
Protection of children, and women and girls	
Safeguarding children is a core aim of the OSA. The Act, and in particular Ofcom's supplementary consultation documents, guidance and codes of practice for this specific aim contain detailed provisions for platforms accessible by children, including duties to conduct risk assessments and implement proportionate measures to tackle content that is harmful to children (including specific harms set out in the legislation). The OSA uniquely makes provision for Ofcom to issue specific guidance on content and activity which disproportionately affects women and girls. This is in recognition of Ofcom's research showing that women and girls are more negatively affected by hateful and trolling content, feel less able to have a voice and share their opinions online, and are also disproportionately affected by certain kinds of online harms, such as intimate image abuse, cyberflashing, and controlling or coercive behaviour. Ofcom published its first consultation and draft guidance on this son 25 February 2025.	The DSA similarly recognises the importance of protecting children, however its obligations are less specific and detailed compared to the OSA. The DSA's express obligations for safeguarding children are mainly set out in Article 28 DSA, which requires that online platforms accessible to minors shall put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors on their service. This Article also prohibits online platforms from targeting adverts to children based on profiling. For VLOPs and VLOSEs, their mandatory risk assessments under the DSA must consider risks to children's rights as enshrined in the UN Convention on the Rights of the Child, and must result in the implementation of targeted risk measures to mitigate those risks, such as age verification and parental control tools. The DSA does not have provisions that are specific to the protection of women and girls.

OSA	DSA
Risk assessments	
Under the OSA, all services in scope must undertake risk assessments. While the DSA has a single type of risk assessment requirement for VLOPs and VLOSEs, the OSA requires different assessments, including risk assessments, to be carried out depending on the category of service. These include: • **illegal content risk assessment** • **children's risk assessment** • **children's access assessment** • **adult user empowerment risk assessment** (for **Category 1** services) Each assessment must be conducted within three months beginning with the day on which the final version of the relevant Ofcom guidance document is published.	Under the DSA, only VLOPs and VLOSEs are required to undertake risk assessments. These assessments must identify, analyse and assess any systemic risks in the EU stemming from the design or functioning of their services, or from the use made of their services. The risk assessments must be specific to their services, and include consideration of certain types of systemic risks set out in the DSA. Assessments must be made within four months of designation as a VLOP/VLOSE, at least annually thereafter, and in any event prior to deploying functionalities that are likely to have a critical impact on the identified risks.
Guidance and codes of practice	
How the OSA's rules take effect in practice is shaped by guidance and codes of practice issued by Ofcom in its statements. These codes and guidance are first issued as draft documents which are published as part of a public consultation. Ofcom is issuing these documents according to three main phases: • Phase one (illegal harms duties) • Phase two (child safety, pornography, and protection of women and girls) • Phase three (duties on categorised services) Ofcom has also been issuing guidance documents which are not phase specific, such as its guidance on Age Assurance and OSA Fees and Notification. This provides a detailed level of information regarding compliance requirements and expectations. While adherence to the codes of practice is not mandatory, following them offers a "safe harbour" for compliance with the OSA's requirements, meaning that compliance is essentially guaranteed. Different OSA compliance deadlines are also expressly tied to the day on which the final version of the relevant Ofcom guidance document is published.	In contrast, the DSA's obligations are much more self-contained in the Act itself and, in particular, within its recitals. The European Commission, the European Board for Digital Services and EU Member State regulators may issue guidance to support service providers with compliance, but the DSA is not structurally driven by guidance and codes of practice in the same way as the OSA. EU Member States may also supplement the DSA with their own national laws and codes, for example Ireland's Online Safety and Media Regulation Act 2022, and Coimisiún na Meán's (Media Commission's) accompanying Online Safety Code.

Enforcement

OSA

Ofcom's enforcement powers will include extensive information gathering powers, including to enter, inspect and audit business premises and to interview an organisation's staff. Further, Ofcom will have the power to impose significant fines of up to £18 million or 10% of qualifying worldwide revenue, whichever is greater. Note that criminal liability for certain infringements of the OSA will also be possible, and in certain circumstances, senior management may face personal liability.

In very serious cases of non-compliance, Ofcom will be able to exercise some invasive, and perhaps quite unusual, 'business disruption' powers, which may require third parties (e.g., payment or advertising providers) to withdraw from their engagement with the provider of the breaching services.

DSA

The DSA similarly gives regulators information gathering and inspection powers, and the ability to order against and sanction service providers (including to request temporary suspension of the service in the case of persistent infringements causing serious harm). Fines under the DSA are up to 6% of worldwide annual turnover in the preceding financial year. There are no specific criminal offences created by the DSA but they may exist under supplementary national Member State laws. Private civil claims in Member State courts are also possible.

Unlike for the OSA, where guidance, supervision and enforcement comes from a single regulator (Ofcom), the pan-EU nature of the DSA means that it gives different roles to multiple different bodies. These include:

- **European Commission**: acts as the top level regulator and has direct investigation and enforcement powers in respect of VLOPs and VLOSEs
- **Digital Services Coordinators**: the Digital Services Coordinator is the lead competent authority responsible for its jurisdiction
- **Additional competent authorities**: while each Member State must designate one DSC as its lead, overall DSA regulator, it may also designate additional competent authorities who regulate specific aspects within their area of expertise. For example, for Ireland, the DSC is Coimisiún na Meán (Media Commission, or CnaM), and its Competition and Consumer Protection Commission is a competent authority with specific responsibility for online marketplaces
- **European Board for Digital Services**: has a supervisory and guidance role, including publishing reports on systemic risks for VLOPs and VLOSEs

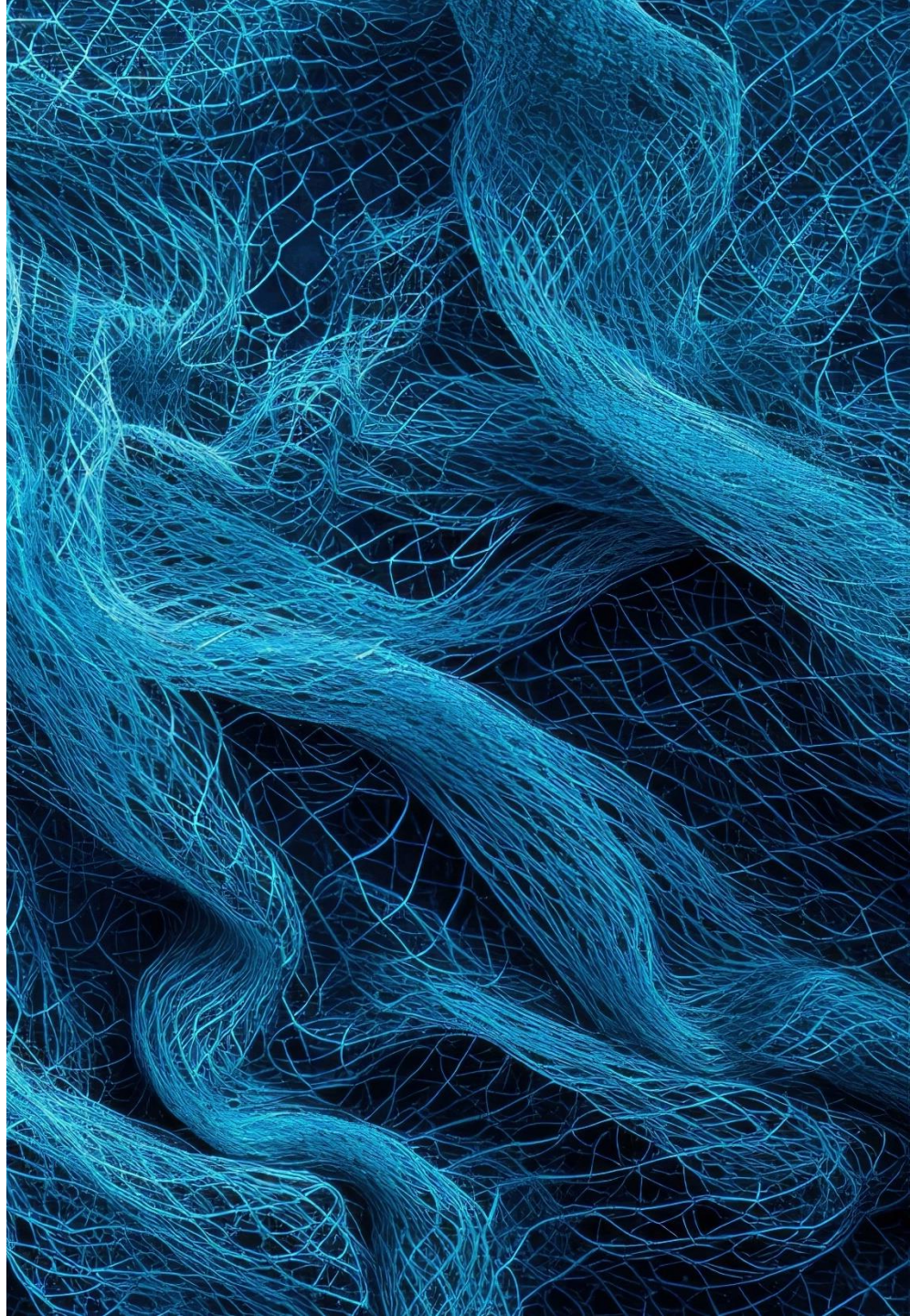
Bristows

Get in touch

If you would like any advice or further information regarding the OSA, please check out our dedicated OSA hub:
The Safety Net

Faye Harrison
Of Counsel
Visit profile
Email

Mike Edgar
Senior Associate
Visit profile
Email



bristows.com