Bird & Bird

EU & UK Online Safety Legislation – a Stocktake

October 2024

Bird & Bird

Contents

A Guide to EU & UK Online Safety Legislation

In this guide we take stock of the two major pieces of online safety legislation in Europe: the Digital Services Act (**DSA**) in the EU and the Online Safety Act (**OSA**) in the UK. We compare and contrast their scope and obligations and assess what, in concrete terms, they are likely to require of the different kinds of **intermediary service providers** within their respective scopes.

What is an "intermediary service"?

Here, we refer to services which play a role in the transmission, storage and/or dissemination of user-provided/generated content – although we have expanded on the different definitions in the DSA and OSA below.

Authors

Graham Smith

Of Counsel

+442074156054
graham.smith@twobirds.com

Heather Catchpole

Associate

+442030176971
heather.catchpole@twobirds.com

What are the DSA and OSA?

History

Common parentage: The OSA and the DSA are close siblings - not twins, but conceived from the same antecedents and with broadly similar aims: to impose positive regulatory duties on certain online intermediaries.

The two pieces of legislation have been running on parallel paths, with the DSA incrementally ahead: the DSA originally proposed by the European Commission in July 2019, and the first draft of the OSA proposed in May 2021, picking up the promises of the UK government's Online Harms White Paper of April 2019.

Growing up at different rates: The DSA overtook the OSA in the race to the statute book, adopted as an EU Regulation in October 2022. The OSA did not receive Royal Assent until 26 October 2023.

Furthermore, the DSA came into effect in short order, with obligations applicable to the largest services (very large online platforms, or VLOPs; and very large online search engines, or VLOSEs) since August 2023 and on other in-scope services since February 2024. The OSA duties, however, become effective only after lengthy consultation by Ofcom, adoption of codes of practice and guidance, and enactment of various items of secondary legislation.

Penalties

Fines under the **DSA** are up to **6% of annual worldwide turnover** in the previous financial year. There are no specific criminal offences created by the DSA but they may exist under national supplementary legislation. Private civil claims in Member State courts are also possible for breaches of DSA obligations.

Fines under the **OSA** are up to **£18 million** or **10% of global annual revenue**. The OSA also creates new criminal offences relating to: false CSEA reporting; conduct in responding to Ofcom's information, enforcement, and audit powers, and new "communications offences" by users. Some offences create criminal liability for corporate officers when there has been consent, connivance or neglect.

B&B Resources: See **Bird & Bird's DSA and OSA implementation tracker here**, which sets out the supplementary Member State laws that could create further penalties for your business. You will also find the status of implementation in each Member State and local contacts for online safety in each Bird & Bird office.

Intermediary liability – history and adjusted shields

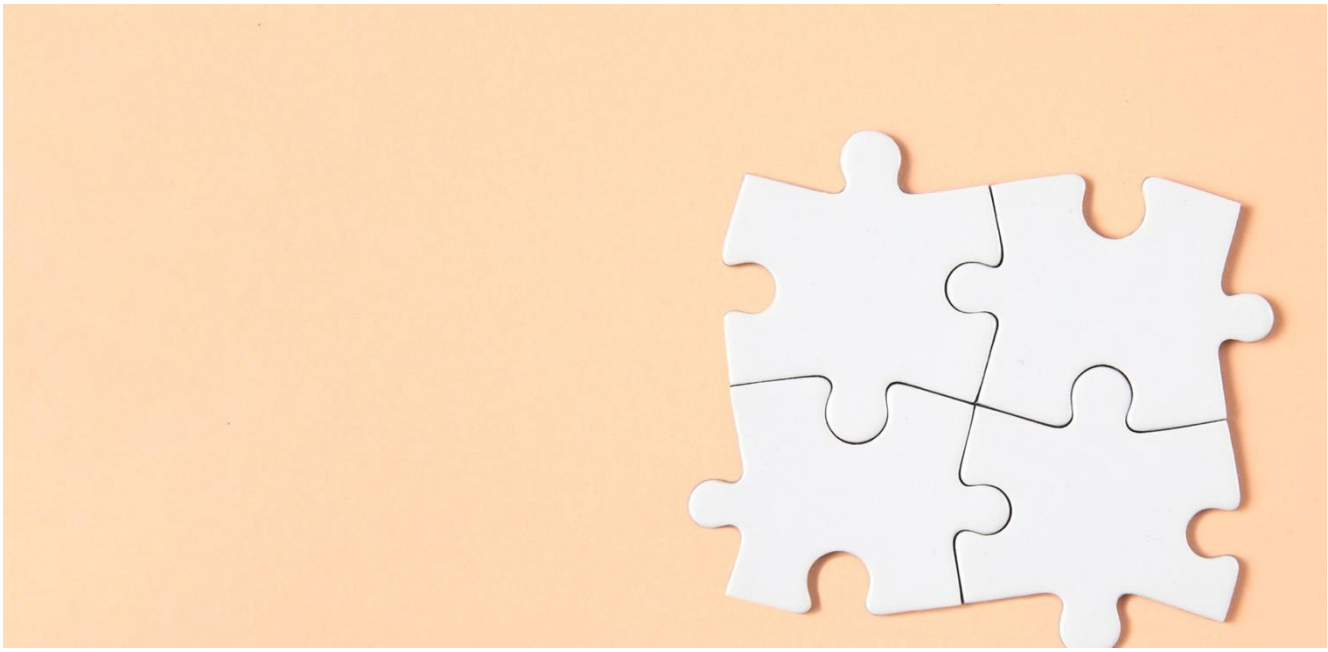
The ECommerce Directive and its liability shields: The DSA and the OSA share a common heritage in the 2000 EU eCommerce Directive (**ECD**).

If you provide an intermediary service, understanding how the DSA and OSA approach the ECD '**notice and takedown'** regime is important to guide you in understanding your risk in relation to specific pieces of user content on your service.

What are the liability shields? In the late 1990s, there was widespread debate about what was, or should be, the liability position of online intermediaries for unlawful user content. With Member States starting to legislate for themselves, the European Commission proposed a harmonised set of graduated liability shields for (i) mere conduit, (ii) caching and (iii) hosting services. These were conceived as a separate protective layer sitting above national laws. An intermediary would benefit from the liability shield if its activity satisfied the relevant conditions. However, if it lost the benefit of the shield, it would not be automatically liable if that content amounted to a criminal or civil offence. Liability would then be a matter for the underlying substantive national or EU law in question, whether that be defamation, copyright, obscenity, or (with a few prescribed exceptions) any other variety of civil or criminal law.

The hosting shield was probably the most significant of the three, since it covered the broadest range of services – discussion forums, social media, cyber-lockers, website hosting, online gaming and many others. Hosts were treated in much the same way as real-world bookshops: liable only if they had relevant knowledge of unlawful content and did not remove it expeditiously upon gaining such knowledge. For criminal liability actual knowledge was required, but for damages an awareness of facts or circumstances from which the unlawfulness was apparent sufficed.

The ECD regime thus incentivised, but did not of itself mandate, what became known as '**notice and takedown'**.



Because the premise of the ECD liability shields was that the user had posted or stored something unlawful, that defined the boundaries of their scope. The ECD had nothing to say about liability for 'lawful but harmful' content, for the simple reason that if user content was lawful there was nothing for which the intermediary could be liable.

How the OSA and DSA deal with the shields

The OSA and DSA do not address the ECD's shields in the same way.

DSA	OSA
The DSA has carried across the ECD's shields and retains the same principle of specifying conditions that must be met to benefit from a shield. The shields act as horizontal, across-the-board, overlays on individual substantive national laws, which are left intact. There are some ways in which the DSA elaborates on the shields – for example, at Art 6(3) DSA, a principle is borrowed from CJEU consumer protection case law to ensure that intermediaries will not benefit from the hosting shield where user content is presented as the provider's own; Art 7 allows "good Samaritan" own-initiative investigations to be undertaken without causing a shield to be lost. In an important addition, notices received by hosting services in the form prescribed by Art 16 DSA will be considered to give rise to actual knowledge or awareness for the purpose of the hosting shield (provided that a diligent provider of hosting services could identify the illegality without a detailed legal examination). This puts additional pressure on hosts to review and respond to the notices they receive through the new mechanism.	The OSA has not touched the ECD liability shields. Prior to Brexit, the shields were implemented through a variety of legislation, including the UK's Electronic Commerce (EC Directive) Regulations 2002 (**eCRs**). The existing shields remain in force and therefore coexist with the OSA. However, as a result of the way in which the eCRs adopted the ECD shields into UK law, the shields will not be automatically updated where new offences and liabilities are enacted by the UK Parliament. Proactive effort is required by the UK legislator to extend the shields. Legislation-specific carveouts from liability (as, for example, for the new Communications Offences in the OSA) may also exist. This adds an additional element of uncertainty to the UK shield regime.

The truly new: "positive" obligations on intermediaries

Where both the DSA and the OSA break newer ground is in imposing positive obligations, supervised and enforced by a regulator, on various kinds of online intermediaries in relation to the harms posed by the content on their services. These obligations apply irrespective of the protection of the ECD shields.

This means that even if an intermediary fulfils all the criteria of the relevant shield, such that it has a defence from liability under national criminal or civil law for particular piece(s) of content, it could still be in breach of a regulatory obligation imposed by the DSA or OSA. This results in a significant increase in risk profile for providers of intermediary services.

For more information on the specific positive obligations the DSA and OSA have created, see our section on "DSA vs OSA – key thematic differences" below.

Other content laws

The DSA and OSA do not govern online safety in a vacuum. For example, there are other EU laws affecting online intermediaries which are specific to particular sectors or types of illegal content. Notable examples include the EU Terrorist Content Online Regulation (**TCOR**), the (upcoming) EU CSAM Regulation, and the Audiovisual Media Services Directive (which has been implemented nationally in each Member State/in the UK prior to Brexit).

Are we in scope?

Extraterritoriality

The DSA and OSA follow the trend in recent digital and online safety legislation of having extra-territorial scope. If you are established outside of the EU or UK respectively, there is therefore still a likelihood that these regulations will be relevant. It is likely that "targeting" criteria in particular may be interpreted in line with previous EU and UK case law.

DSA	**OSA**
Requires a "substantial connection" to the EU – including (where no EU establishment) having a "significant number" of recipients in a Member State, or the targeting of activities towards a Member State.	Requires a "UK link" – including (where no UK establishment) a "significant number" of UK users or having the UK as a target market. In addition (with no equivalent in the DSA), this may be satisfied by a service being capable of use in the UK and its content posing a "material risk of significant harm" to UK users. This could potentially capture services which do not intentionally target the UK but have particularly risky content.

Service categorisation

The DSA and OSA differ markedly as regards which services are in scope and the nature and subject matter of the obligations.

We look first at the differences in scope, which have to be considered on a service-by-service basis. One Act cannot be said to be, as a whole, "broader" in scope than the other – rather, different aspects of scope are broader or narrower.

DSA		**OSA**
Only "ISSs" in scope Intermediary services under the DSA must be a type of "information society service" or "ISS". Part of this definition requires that the service is "normally provided for remuneration". However, this tends to be liberally interpreted.		**Possible application to non-commercial services** The OSA applies to both commercial and non-commercial services.
Intermediary services Nominally the DSA applies to	**Mere conduit** – transmission in a communication network of recipient-provided information,	**"User to user"** The OSA, in contrast, starts from scratch with homegrown definitions. Its definition of user-to-user (**U2U**) services requires the

<table>
<tr><th colspan="2">DSA</th><th>OSA</th></tr>
<tr><td rowspan="4">intermediary services (and thus to the examples given) only to the extent that they are engaging in either conduit, caching or hosting activities, adopting the terminology from the ECD.</td><td>or provision of access to a communication network - ISPs, direct messaging, VPNs.</td><td rowspan="4">possibility of user-generated content being “encountered” by another user(s) of the service. Subject to exemptions, this is likely to capture most DSA online platforms. For DSA-caught services, a careful analysis will be required as to whether they have a U2U element that is not otherwise exempt (see below).

To illustrate the breadth of the OSA U2U definition, the Ofcom Illegal Harms Consultation lists various kinds of in-scope services: social media, video-sharing, messaging services, marketplaces, listing services, dating services, review, gaming, file-sharing, audio sharing, discussion forums and chat rooms, information sharing sites, crowdfunding sites, user-generated adult entertainment sites.

A special regime still applies to video-sharing platform (VSP) services in the UK. Pre-existing UK-established VSPs were already subject to a degree of online safety supervision by Ofcom under the UK’s implementation of the EU Audiovisual Media Services Directive, and are now “transitioning” over to the OSA regime. New VSPs in-scope of the OSA who only started providing services on or after 10 January 2024 will only be regulated by the OSA.</td></tr>
<tr><td>Caching – transmission in a communication network of recipient-provided information, but with an additional element of automatic, intermediate and temporary storage for the sole purpose of making the onward transmission of the information to other recipients upon their request more efficient - Content delivery networks, content adaptation proxies.</td></tr>
<tr><td>Hosting – storage of recipient-provided information at their request - Cloud storage, cloud-hosted messaging, but also...</td></tr>
<tr><td>Online platform (subset of hosts) – hosting and also, at a recipient’s request, dissemination of that information to the public - Social media, public forums, some online games, marketplaces (with specific obligations for B2C marketplaces), dating apps, app stores, review-sharing websites.</td></tr>
</table>

DSA	OSA
Exemptions SMEs are exempt from transparency reporting and online platform-specific obligations. Where a hosting service has online platform functionality but this is only a "minor and purely ancillary feature" of an overall service, this will be exempt from an online platform categorisation.	**Exemptions** The OSA service exclusions are a disparate but important collection: e-mail, SMS/MMS, one-to-one live aural communications, reader comments on news items (where user replies to such comments are not permitted), reviews relating to provider content (again, where user replies to such reviews are not permitted), internal business tools and resources, certain public body services, and certain education and childcare provider services.
Search... Search engines were never conclusively established under the ECD to involve any mere conduit, caching or hosting activities, as is required by Art 3(g) DSA for a service to qualify as an "intermediary service". Art 21 of the ECD mentioned the need for future proposals concerning the liability of search engines, but these never materialised. However, the language and purpose of the DSA, especially given the existence of VLOSEs, suggest that search engines are in scope. Search engines are defined as services that "must be able to perform searches of, in principle, all websites, or all websites of a particular language".	**Search** Search engines fall within scope of the OSA, and only search engines which only search *one* website or database are excluded. This means that, as well as general-purpose search, vertical search services such as sector-specific price comparison sites will be in-scope of the OSA (but not the DSA). It is possible for services to be "combined" services – i.e. containing both a search engine and a U2U element.
Very large services The highest level of obligations apply to VLOPs and VLOSEs. The DSA defines these categories by size alone (an average of 45 million monthly active users in the EU).	**Categorised services** The OSA delegates categorisation thresholds to secondary legislation, with thresholds to take into account both risk and size and Ofcom's advice. Like VLOPs and VLOSEs, categorised services have enhanced (but different) duties from other entities caught by the OSA.
Severability of service It is possible to carve out different technical functionalities of an intermediary service and for them to have different DSA	**Severability of service** The same principles from the DSA are likely to apply in the OSA. The OSA expressly confirms that it is possible for

DSA	OSA
categorisations. However, for the purpose of e.g. disclosing user numbers (which is an obligation for online platforms), if the user base cannot be severed because there is no separation in a user's experience, then all users may need to be counted together as part of a single regulated online platform service.	only a discrete or peripheral part of a service to be in-scope because of its U2U/search functionality. However, when assessing whether a service is categorised based on user numbers, for example, it may be too challenging to sever elements of an overall service when counting users.
Who is the "provider"? The DSA does not have a definition of a service provider, although "terms and conditions" are defined as the contractual terms between the service provider and recipient, meaning this will be indicative of the provider entity. Where an intermediary service subcontracts any element of intermediation (e.g. cloud hosting), *both* would be regulated under DSA.	**Who is the "provider"?** The OSA defines the provider of a U2U service as the entity with control over who can use the U2U part of the service. In addition, "users" exclude bots controlled by the provider and employees/contractors of the provider. The latter may leave some uncertainty around e.g. enterprise video conferencing services where meetings are attended by both employees and external attendees (and, as such, not excluded as an internal service).

Why categorisation matters – it dictates your obligations

Both the DSA and OSA graduate obligations according to the band within which a service has been categorised. Substantially different duties can apply dependent on size and risk.

This graduated approach is why it is so important to categorise your service(s) effectively – it is not possible to determine your obligations without this analysis.

Carefully applied categorisation may mean that you can take advantage of exemptions or move a service "down" to a category with fewer obligations. Practical examples include:

- **User comments on a provider's feed** – provided the comments are not a "minor or ancillary" feature of the overall service, DSA obligations will still apply. However, if the functionality is limited solely to user comments on the provider's content (and not user replies to those comments), an OSA exemption will be available.
- **Instant messaging services** – these services will be subject to many of the U2U obligations under the OSA. However, under the DSA, unless they facilitate public chat channels, they may be able to fall under a mere conduit categorisation with significantly fewer safety obligations.

What do we need to do?

Which content is in-scope?

Insofar as obligations under the DSA or OSA relate to content, the kinds of content are significantly different in each type of legislation.

DSA	OSA
Illegal "Illegal content" covers both civil and criminal liability. The DSA does not set out specific offences that will be covered. Assessments as to whether particular content is illegal are to be made under national Member State laws. There is a body of CJEU case law dealing with when providers will have "actual knowledge" or "awareness" of illegality.	**Illegal** Illegal content under the OSA *only* covers certain criminal offences (with some excluded offences in the areas of IP, safety/quality of goods, services by unqualified persons and consumer protection). As above, some content is also excluded by virtue of the exemptions. A subcategory of "priority illegal content" is defined by reference to specific UK criminal offences and is relevant to the extent of providers' obligations in respect of that content. The OSA acknowledges that providers would need to make their own judgments as to whether content is illegal content. The OSA's test is "whether a provider has *reasonable grounds to infer* that content is illegal", on which Ofcom has produced guidance.
Legal but harmful Harmful content is not generally covered by the DSA's requirements. However, for VLOPs/VLOSEs only, their "risk mitigation" duties could extend to harmful content too, whilst online platforms "accessible to minors" have safety duties in relation to minors which could arguably extend to harmful content (though this is not specified).	**Legal but harmful** This was a much-debated aspect of the OSA. Certain, but now only limited, duties extend to legal but "harmful" content including the children's risk assessment/mitigation duties and Category 1 services' adult user empowerment duties, which require services to give adults control over certain types of content they may see. "Harm" is defined as "physical or psychological harm" and may arise as presented by, or in relation to, content.

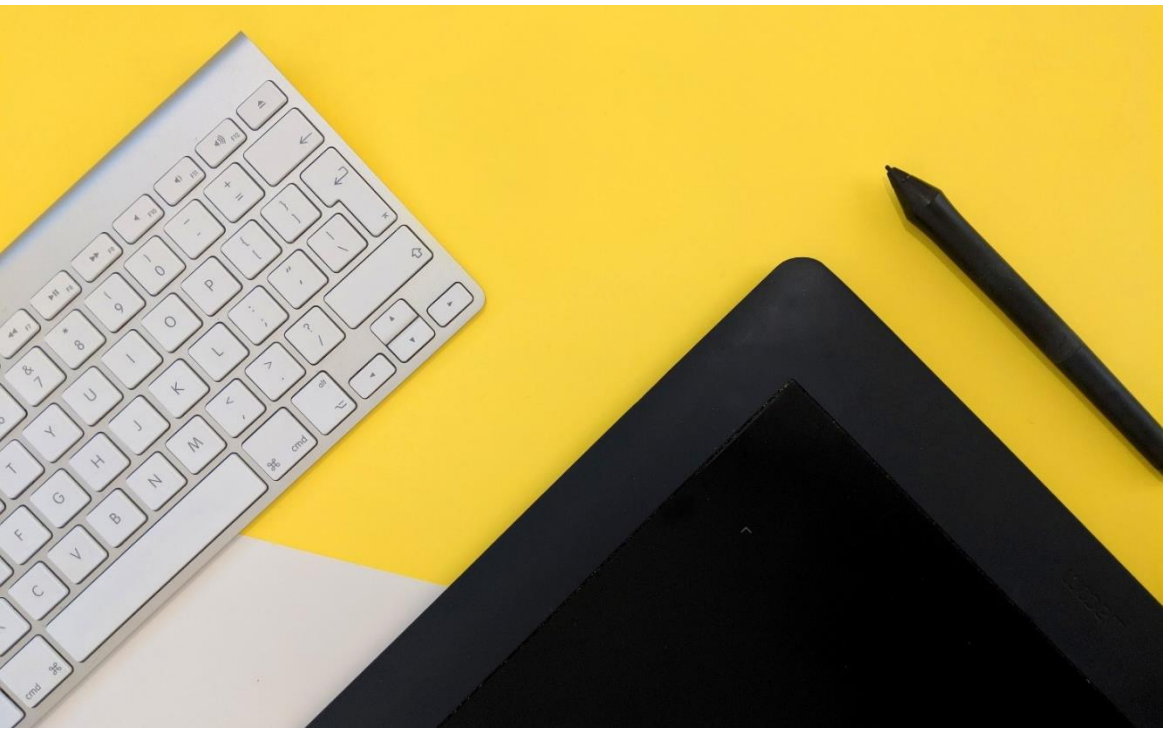
Designing an implementation programme

In practice, given timings (with the DSA having become applicable first) and the fact that the EU is likely to be a larger user base, many services will begin or have already begun by implementing the DSA and then turning to the OSA, hoping that some DSA safety measures could be carried across for OSA compliance. Most services have been doing this by way of a "gap analysis" and we have provided guidance on the key differences between the legal duties of each Act below.

Other considerations are:

- **Interaction with privacy and data protection obligations** – in particular, you may have already implemented some measures under children's privacy guidance like the Age-Appropriate Design Code (**AADC**) in the UK, or taken account of the UK Information Commissioner's Office's guidance on content moderation and data protection. It is crucial to make sure your online safety stance aligns with any stances taken, particular in discussion with regulators.
- **Informing product teams** – brief product teams to factor the DSA/OSA review into product timelines well in advance.
- **Work done in other jurisdictions** – online safety regimes also exist in (for example) Australia and Singapore; if your service is global, be in touch with those teams to determine the steps they have already taken or whether DSA or OSA measures can be repurposed there as well.

B&B Resources: See our Bird & Bird teams' summaries of the **Australian** and **Singaporean** online safety regimes here and here; the UK's groundbreaking **AADC** here; and the UK Information Commissioner's **guidance on content moderation and data protection** here.



"DSA vs OSA" – key thematic differences

We have set out key themes to consider as part of any gap analysis below (for the OSA, these examples relate to U2U services, but there are minor differences for search services).

For the **OSA**, a provider's obligations will be heavily dependent on both the outcome of its risk assessment and the content of Ofcom's finalised codes of practice. Businesses can take a "comply or explain" approach to the codes, i.e. there is no legal obligation to implement Ofcom's recommended measures, but any divergent attempt to meet OSA duties by alternative means needs to be justified and documented. Conversely, a provider who adopts all the measures recommended to a service of their size and risk profile in a code of practice is deemed to satisfy the corresponding duties imposed by the OSA.

For the **DSA**, there are detailed requirements around some provisions in particular (such as notice & action) but others, particularly minor safety for online platforms and VLOP/VLOSE risk mitigation, are left much broader and are subject to subsequent guidance.

DSA	**OSA**
Risk assessment **Only** VLOPs and VLOSEs need to conduct risk assessments under the DSA. DSA risk assessments are cast in much broader and vaguer terms than under the OSA, requiring that VLOPs and VLOSEs "identify, analyse and assess any systemic risks in the Union stemming from the design or functioning of their service". Online platforms (both VLOPs and non-VLOPs) also have a broadly-couched minor protection duty – in practice, this may well require an assessment of risk in order to determine which measures are appropriate.	**Risk assessment** In perhaps the key difference from DSA compliance work, **all** OSA services need to complete an illegal content risk assessment, and a child's access assessment to determine whether they are likely to be accessed by children (U18s). Services that pass the child's access assessment (which will be the vast majority of U2U services unless they can clearly evidence that children are unlikely to access their service) will also need to conduct a children's risk assessment. Additional risk assessments will follow for Category 1 services, in relation to user empowerment duties.
Content moderation Mere conduits and caches are not obliged to undertake any specific kind of content moderation but, to the extent they do, it will impact their other obligations around e.g. T&Cs and transparency reporting. In addition to the above, hosting services *will* need to implement reactive "notice & takedown" flows in order to preserve their liability shields.	**Content moderation** The OSA imposes an obligation to have a system or process designed to remove illegal content of which the provider becomes aware swiftly. This is a self-standing duty that applies independently of a service's risk assessment outcome. Services can likely borrow heavily from any DSA notice & action mechanism in this regard, although different types of content may be relevant.

DSA	OSA
Unlike the OSA, however, which can require proactive content detection, the DSA cannot require a provider to engage in general monitoring of the information provided or stored by its users. This is one of the most significant differences between the DSA and the OSA.	Any further proactive moderation measures are left to Ofcom's codes, and are not constrained by a prohibition equivalent to the one in DSA on the imposition of general monitoring requirements. At the time of writing, in its Illegal Harms Consultation Ofcom has already recommended some forms of proactive moderation – CSEA hash matching, CSEA URL matching, and fraud keyword matching – for some services, depending on their size and risk. Uniquely, and controversially, the OSA also confers on Ofcom the power to require U2U platforms to install technology to scan for terrorist and CSEA content (on publicly-posted content) and CSEA content (on private messaging platforms). This has led to concerns that a messaging service might be prevented from deploying end-to-end encryption if it impeded the use of the required technology. Although some safeguards are implemented in the OSA and although the UK Government has indicated that appropriate technology must first be developed for the exercise of this power to be possible, it remains controversial that the reference to private communications has remained in the Act.
Transparency & user tools **All** DSA services need to complete annual (or for VLOPs/VLOSEs, every six months) transparency reports in a prescribed form. **All** DSA online platforms also need to publicly disclose their monthly average user numbers every six months. The DSA includes additional obligations around updates to (and the consistency of the application of) terms and conditions, and transparency in an adtech context. Any remaining transparency/user tool-related recommendations are left to	**Transparency & user tools** **Only** Categorised services need to submit transparency reports under the OSA. Their format is more flexible than under the DSA and will be dictated by the content of Ofcom's transparency notices. For **all** in-scope U2U services, similar requirements around terms and conditions to those in the DSA apply, and terms must additionally be prescriptive as to how the different types of the OSA's priority illegal contents are dealt with. User tools and default settings for children are likely to play a role in Ofcom's recommended safety measures. The OSA also requires Category 1 U2U providers to

DSA	OSA
upcoming regulatory guidance on risk mitigations.	provide adults with 'user empowerment tools' enabling them to see less of, or be alerted to, legal but harmful content.
Additional focus areas – adtech, dark patterns and the protection of minors (guidance to come) The DSA's adtech-related provisions extend to prohibiting targeting based on special category/minors' data and requiring VLOPs/VLOSEs to put in place searchable "ad repositories". The DSA also bans "dark patterns" (though not to the extent covered already by GDPR/consumer law). Dark patterns are not mentioned in OSA. Art 28 DSA contains a broad minor protection duty, which will be subject to further guidance.	**Additional focus areas – age assurance and recommender systems** Ofcom's codes will recommend age assurance for the purposes of restricting access to either particular content or the entire service (with guidance on what is considered "highly effective age assurance"), and will propose measures relating to recommender system algorithms.
Governance **All** DSA services need to appoint point(s) of contact for both service recipients and authorities. Non-EU established services need to appoint a DSA representative in the EU, who can be liable under the DSA for the provider's infringements.	**Governance** Ofcom's final codes are likely to recommend measures around named and internally accountable individuals. Ofcom also has powers to serve information notices requiring notification of a senior manager responsible for complying with the notice. There is no formal representative requirement, however.

B&B Resources See Bird & Bird's easily navigable index of OSA obligations here and our webpage here (which sets out guidance and enforcement at the time of writing), to assist with the interpretation of the obligations described above.

Your B&B Online Safety team

B&B's Online Safety lawyers

For legal assistance with your DSA and OSA compliance, reach out to a member of our Online Safety team. We can help with:

- Scoping and service categorisation
- Risk assessments
- Gap analysis
- Regulatory engagement
- DSA/OSA audits

A number of our lawyers also practice in closely aligned areas such as privacy, consumer and telecommunications law, and are well-placed to bring cross-practice insights.

Your UK team

Graham Smith

Of Counsel

graham.smith@twobirds.com

Emma Drake

Partner

emma.drake@twobirds.com

Heather Catchpole

Associate

heather.catchpole@twobirds.com

Shona O'Connell

Senior Associate

shona.oconnell@twobirds.com

Matthew Buckwell

Senior Associate

matthew.buckwell@twobirds.com

Maureen Coen

Associate

maureen.coen@twobirds.com

twobirds.com

Abu Dhabi • Amsterdam • Beijing • Bratislava • Brussels • Budapest • Casablanca • Copenhagen • Dubai • Dublin • Dusseldorf • Frankfurt • The Hague • Hamburg • Helsinki • Hong Kong • London • Lyon • Madrid • Milan • Munich • Paris • Prague • Rome • San Francisco • Shanghai • Shenzhen • Singapore • Stockholm • Sydney • Warsaw