# Mind the gap: Content Moderation in UK vs. EU

Comparing and contrasting the EU and UK approach to content moderation under the DSA and OSA. By **Shóna O'Donovan** and **Madelaine Harrington** of Covington & Burling LLP.

Tackling illegal and harmful content online is a priority for many countries—and their citizens—globally. The EU and UK are no exception. In recent years, both jurisdictions have introduced new laws, the EU's Digital Services Act (DSA) and the UK Online Safety Act 2023 (OSA), which impose rules on providers of services that host user-generated content (UGC) to remove or limit the reach of illegal and, in some cases, legal but "harmful", UGC on their services.

Prior to introducing the DSA and the OSA, both the EU and UK primarily relied on the safe harbour framework established by the eCommerce Directive (eCD) to address illegal UGC online, with some additional rules for video-sharing platforms under the Audiovisual Media Services Directive. Although both jurisdictions were working from broadly this same starting point, the DSA and OSA take very different approaches to further regulating services that host UGC.

This article will provide an overview of the key differences and similarities between the DSA and the OSA across a range of topics, including terms and conditions on content moderation, how "illegal content" is defined under each Act, government orders to remove content, risk assessments, content moderation and minors and enforcement.

> Both the DSA and the OSA impose obligations on in-scope providers to address "illegal content" on their services, but they define those terms somewhat differently.

## Approaches taken by DSA and OSA

The DSA and the OSA apply to a range of services; however, this article will focus only on services that host and disseminate UGC online. In that regard:

- The DSA applies to "hosting services"—that is, a service "consisting of the storage of information provided by, and at the request of, a recipient of the service" (Art. 3(g)(iii)). This definition encompasses "services enabling sharing information and content online, including file storage and sharing" (Rec. 29). The DSA also applies additional rules to a subset of hosting services called "online platforms". These are hosting services that, "at the request of a recipient of the service, store and disseminate information to the public" (Art. 3(i)) such as, social media services, online marketplaces and photo- and video-sharing services.
- The OSA, on the other hand, applies to "user-to-user" (U2U) services—namely, services through which users may "encounter" UGC (s. 3(1)). This captures many of the same types of services as "hosting services" and "online platforms" under the DSA. It also includes many instant messaging services that may not always come within the DSA's scope, such as app-based messaging services.

**Terms and conditions on content moderation**: The DSA obliges all hosting providers to include, in their terms and conditions with users, "information on any restrictions that they impose" on UGC (Art. 14(1)). That information must include information on any "policies, procedures, measures and tools used for the purpose of content moderation including algorithmic decision-making and human review" (id.). The DSA mandates that providers act in a "diligent, objective and proportionate manner" when applying and enforcing any restrictions on UGC, and pay "due regard" to the fundamental rights of users, "such as the freedom of expression, freedom and pluralism of the media, and others" (Art. 14(4)).

The OSA also imposes obligations — known under the OSA as "duties of care" — on U2U providers to include information on content moderation efforts in their terms of service, although the focus of those duties is somewhat different. Specifically, the OSA imposes a duty on U2U providers to explain, in their terms of service, how individuals will be "protected from" illegal content on the service (s. 10(5)), and providers must apply these provisions "consistently" (s. 10(6)). U2U providers must also provide information to users about any "proactive technology" used to comply with their duties, including information on "the kind of technology, when it is used, and how it works" (s. 10(7)). The OSA applies similar obligations on providers of U2U services "likely to be accessed by" children (i.e., under 18s) with regard to content that is legal, but "harmful to children" (see "Approach to content moderation for minors" for more information).

**Definition of "illegal content"**: Both the DSA and the OSA impose obligations on in-scope providers to address "illegal content" on their services, but they define those terms somewhat differently.

The DSA defines "illegal content" as any information that "is not in compliance with" EU or Member State law, "irrespective of the precise subject matter or nature of that law" (Art. 3(h)). This definition encompasses both content that is criminal in nature

(e.g., terrorism content, child sexual exploitation and abuse material (CSEA), and content that is not criminal, but infringes EU or Member State law, e.g., "the sale of products or the provision of services in infringement of consumer protection law, the non-authorised use of copyright protected material, the illegal offer of accommodation services or the illegal sale of live animals" (Recital 12).

By contrast, the OSA's definition of "illegal content" is more squarely focused on content that is criminal in nature—it is content that amounts to a "relevant offence" (s. 59(2)). "Relevant offences" encompass terrorism offences (Schedule 5), CSEA offences (Schedule 6), a wide range of interpersonal offences (e.g., threats to kill, harassment, stalking—see Schedule 7) and offences where "the victim or intended victim is an individual (or individuals)" (s. 59(5)(b), emphasis added).

**Orders to act against illegal content**: Although the DSA does not specifically empower governmental authorities to issue orders to in-scope providers to act against illegal content, it does oblige providers who receive such an order to inform the issuing authority "of any effect given to the order without undue delay, specifying if and when effect was given to the order" (Art. 9). By contrast, OFCOM, the OSA regulator, has stated that its role "isn't about deciding whether particular posts or other content should or shouldn't be available, or whether it complies with specific standards"—rather, it is focused on ensuring that U2U providers have "appropriate systems and processes in place to protect their users."[1]

**Notice and action mechanisms**: One of the cornerstone obligations the DSA imposes on hosting service providers is to implement a "notice and action mechanism" – i.e. a mechanism to allow individuals to notify the provider of the presence of any content they suspect to be illegal on the service (Art. 16(1)). Notices must include clear details including why the content is illegal, where it is located (such as the exact URL), the notifying party's contact information, and a statement from the notifying party confirming that the allegations in the notice are accurate and complete (Art. 16(2)). Importantly, if a notice contains all the required elements, it is presumed to give the provider "actual knowledge" of the illegal content (Art. 16(3)). This is important because hosting services are only liable for illegal UGC once they become aware of it.

The OSA requires all U2U providers to operate their services "using proportionate systems and processes" to "minimise the length of time for which" any "priority illegal content"—that is, terrorism content, CSEA content or content that amounts to a Schedule 7 offence— is present on the service. Further, where the U2U becomes aware of such content on their service, they must "swiftly take [it] down" (s. 10(3)(a)-(b)). The OSA imposes a similar obligation on "Category 1" services with respect to fraudulent ads (s. 38). Although these duties do not specifically oblige providers to implement notice and action mechanisms for this content, in practice, many U2U providers may choose to leverage existing notice and action mechanisms for this purpose.

**Risk assessments/mitigation of risks**: The DSA requires only the largest online platforms—known as "very large online platforms" (VLOPs)— to conduct annual risk assessments to identify and analyse systemic risks stemming from the design and operation of their services. These include among other things risks related to the dissemination of illegal content, negative impacts on fundamental rights, threats to public security, and negative effects on civic discourse or public health, or in relation to gender-based violence or the protection of minors (Art. 34(1)). VLOPs must also publish a report setting out the results of the risk assessments (Art. 42(4)(a)). Based on their assessments, VLOPs must implement proportionate and effective mitigation measures, such as adapting content moderation practices, modifying algorithms, reinforcing internal processes, or adapting product design (Art. 35(1)).

By contrast, the OSA obliges all U2U service providers—and not just those designated as highest risk or having the largest size by OFCOM—to perform an "illegal content risk assessment" (ICRA) to identify and assess the risks on their services associated with illegal content (s. 9), and to "effectively mitigate and manage the risks of harm to individuals, as identified in the most recent [ICRA] of their service" (s. 10(2)(c)). U2U providers are under a duty to keep their ICRAs "up to date," and OFCOM recommends that providers review their ICRAs every 12 months.[2]

**Approach to content moderation for minors**: Under the DSA, providers of online platforms are subject to a general obligation to put in place appropriate and proportionate measures to "ensure a high level of privacy, safety, and security of minors, on their service" (Art. 28(1)). The European Commission will publish Guidelines to support platforms with Article 28 compliance. Draft Guidelines for public consultation were published on 13 May 2025 and include a recommendation to "[i]mplement measures to prevent a *minor's repeated exposure to content that could pose a risk to minors' safety and security*" (lines 551-552, emphasis added).

The OSA, by contrast, imposes specific and relatively detailed duties on U2U providers to address content that is legal, but "harmful to children" on services that are "likely to be accessed by children." Content is "harmful to children" if it is designated as one of the following under the OSA:

- **"Primary priority content"**: This includes pornographic content (s. 61(2)); or content that "encourages, promotes or provides instructions for": suicide (s. 61(3), an "act of deliberate self-injury" (s. 61(4)), or "behaviours associated with an eating disorder" (s. 61(5)).
- **"Priority content"**: This encompasses a wide range of content, including "content which is abusive" and which targets: race, religion, sex, sexual orientation, disability, or gender reassignment (s. 62(2)); content that "incites hatred against" people on the basis "of a particular race, religion, sex or sexual orientation," "disability" or "who have the characteristic of gender reassignment" (s. 62(3)), among others.

Content may also be "harmful to children" if it is not designated under the OSA, but is "of a kind which presents a *material risk of significant*

 

*harm to an appreciable number of children in the [UK]*" (s. 60(2)(c), emphasis added).

Providers of services that are "likely to be accessed by children" are subject to a range of duties of care, including to perform a "children's risk assessment" (CRA) to, among other things, identify the level of risk of child users encountering content that would be harmful to them on the service (s. 11(6)(b)) and to "take or use proportionate measures" to "mitigate and manage" the risks of harm to children on the service "as identified in the most recent [CRA]" (s. 12(2)(a)). Providers of such services must also take steps to "mitigate the impact of harm to children" presented by content that is harmful to children on their services (Section 12(2)(b)). They must also operate their services using "proportionate systems and processes" designed to "prevent children of any age from encountering" primary priority content that is harmful to children (Section 12(3)(a)). This latter duty requires a provider to use "age verification or age estimation (or both)" to prevent children from "encountering primary priority content that is harmful to children which the provider identifies on the service."

## Conclusion

The DSA has applied to all in-scope providers since February 2024, and providers will already have mechanisms in place to ensure compliance. The OSA's duties, however, continue to apply to in-scope providers on a rolling basis; the duties with respect to illegal content started to apply to all U2U providers in March 2025, and the duties that apply to services likely to be accessed by children will apply from July 2025. Companies that are subject to the DSA are likely to be looking to leverage existing compliance mechanisms to comply with the OSA. They may also be looking to review and update their DSA compliance practices to respond to changing guidance or, where the OSA's requirements go beyond the DSA, to apply OSA measures in the EU to ensure as much consistency as possible across jurisdictions. To do that, it will be important for providers to understand the distinctions between the legal requirements under each set of rules.

**AUTHORS**

Shóna O'Donovan and Madelaine Harrington are Associates at Covington & Burling LLP's UK office.
Emails: sodonovan@cov.com
mjharrington@cov.com

**REFERENCES**

1 OFCOM, Online safety – what is Ofcom's role, and what does it mean for you? 9 November 2023. Available at: www.ofcom.org.uk/online-safety/illegal-and-harmful-content/online-safety-ofcom-role-and-what-it-means-for-you
2 OFCOM, Risk Assessment Guidance and Risk Profiles. 16 December 2024. Available at: www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/illegal-harms/risk-assessment-guidance-and-risk-profiles.pdf?v=390984


ESTABLISHED 1987

UNITED KINGDOM REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

# Data (Use and Access) Act 2025 becomes law

The Bill was granted Royal Assent on 19 June.
By **Laura Linkomies**.

The House of Lords passed the Data (Use and Access) Bill on 11 June. Receiving Royal Assent means it is now on the statute books. A long ping-pong between the two Houses about AI training and copyright delayed the last stages of the Bill which had broad cross-party support. The new law does not alter the UK's current data protection regime as dramatically as was proposed under the Conservative government.

Commenting on the relationship

*Continued on p.3*

# Getting it right handling complex DSARs and how AI can help

**Jenai Nissim** and **Claire Saunders** of HelloDPO Law explain how you can use AI to successfully manage data subject access requests – especially in cases that involve large volumes of information.

Even if you have got the basics down to a fine art, a policy and procedures in place, templates and exemptions assessments to help you navigate data subject access requests (DSARs), dealing with a significant DSAR can still be a daunting prospect. In this article, we discuss how you can prepare for the inevitable eventuality of dealing with a DSAR and the assistance that can be provided by technological

*Continued on p.4*



Issue 140 **JULY 2025**



***See the publisher's blog 'A gap between political and legal aspects of new UK law' at privacylaws.com/blog2025jul***

UNITED KINGDOM
report

ISSUE NO 140 **JULY 2025**

**PUBLISHER**
**Stewart H Dresner**
stewart.dresner@privacylaws.com

**EDITOR**
**Laura Linkomies**
laura.linkomies@privacylaws.com

**DEPUTY EDITOR**
**Tom Cooper**
tom.cooper@privacylaws.com

**REPORT SUBSCRIPTIONS**
**K'an Thomas**
kan@privacylaws.com

**CONTRIBUTORS**
**Jenai Nissim and Claire Saunders**
HelloDPO Law

**Richard Jeens, Natalie Donovan and Tayla Byatt**
Slaughter and May

**Conor Moran and Francis Katamba**
Browne Jacobson LLP

**Emma Erskine-Fox**
TLT LLP

**Shóna O'Donovan and Madelaine Harrington**
Covington & Burling LLP

**PUBLISHED BY**
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
**Tel: +44 (0)20 8868 9200**
**Email: info@privacylaws.com**
**Website: www.privacylaws.com**
**Subscriptions:** The *Privacy Laws & Business* United Kingdom Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.
Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2047-1479


# comment

## Data protection and cyber security go hand in hand

The astonishing cyber incident suffered by Marks & Spencer this spring immediately impacted consumers. While the company said it swiftly and proactively took steps to protect its systems, online shoppers experienced major disruption. Some personal data was breached, including contact details, dates of birth and online order history.

M&S said it reported the incident to relevant government authorities and law enforcement and continues to work closely with them. The M&S Chief Executive explained that the criminals had gained access to the retailer's systems via one of M&S's contractors, for example by posing as a staff member. Read an analysis of this cyber attack, including lessons for organisations, on p.10, and an analysis of the forthcoming Cyber Security and Resilience Bill on p.7.

The Data (Use and Access) Act is now on the statute books. As we are going to print, Royal Assent has been granted and secondary legislation will follow (p.1). This was a long legislative process starting with the attempts made by the previous government.

We will report in future issues on the various aspects of this new law which builds on the existing framework rather than radically departs from it. Also look out for our one-day conference in London on the new law on 1 October (p.14). Before that, we'll hear ICO and DSIT speakers talk about various aspects of the law, including how they will enforce it, at our 7-9 July conference in Cambridge (see p.14). You may register for in-person or online attendance.

The UK may be on its own after Brexit but in the data protection world we still look at the EU to understand the reactions of EU DPAs, particularly on novel subjects such as AI. Read on p.12 our correspondent's analysis of the recent fine on a chatbot AI and the aspects that will be worth noting for UK-based data controllers.

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

## Contribute to PL&B reports

Do you wish to contribute to *PL&B UK Report*? Please contact Laura Linkomies, Editor (tel: +44 (0)20 8868 9200 or email: laura.linkomies@privacylaws.com) to discuss your idea, or offer to be interviewed about your organisation's data protection/Freedom of Information work.

# Join the Privacy Laws & Business community

The *PL&B United Kingdom Report*, published six times a year, covers the Data (Use and Access) Act 2025, the UK GDPR, the Data Protection Act 2018, Privacy and Electronic Communications Regulations 2003 and related legislation.

## PL&B's United Kingdom Report will help you to:

**Stay informed of data protection legislative developments.**

**Learn from others' experience through case studies and analysis.**

**Incorporate compliance solutions into your business strategy.**

**Learn about future government/ICO plans.**

**Understand laws, regulations, court and tribunal decisions and what they will mean to you.**

**Be alert to privacy and data protection law issues and tech developments that will affect your compliance and your reputation.**

## Included in your subscription:

**1. Six issues published annually**

**2. Online search by keyword**
Search for the most relevant content from all *PL&B* publications.

**3. Electronic Versions**
We will email you the PDF edition which you can also access in online format via the *PL&B* website.

**4. Paper version also available**
Postal charges apply outside the UK.

**5. News Updates**
Additional email updates keep you regularly informed of the latest developments.

**6. Back Issues**
Access all *PL&B UK Report* back issues.

**7. Events Documentation**
Access *PL&B* events documentation, except for the Annual International Conferences in July, Cambridge.

**8. Helpline Enquiry Service**
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

**9. Free place at a *PL&B* event**
A free place at a *PL&B* organised event when booked at least 10 days in advance. Excludes the Annual Conference. More than one free place with Multiple and Enterprise subscriptions.

**privacylaws.com/reports**

"The UK and International *PL&B* Reports have been my 'go to' resource for 20 years despite the wide choice of alternate resources now available. And have you tried the Annual Conference at Cambridge? I have seven IAPP certificates so a big IAPP supporter. But the *PL&B* Cambridge event each July, still knocks the spots off IAPP and other conferences!"

**Derek A Wynne, SVP Privacy & Chief Privacy Officer, Paysafe Group**

## International Report

Privacy Laws & Business also publishes *PL&B International Report*, the world's longest running international privacy laws publication, now in its 39th year. Comprehensive global news, currently on 180+ countries, legal analysis, management guidance and corporate case studies on privacy and data protection, written by expert contributors

Read in more than 50 countries by regulators, managers, lawyers, and academics.

## Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

## Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.