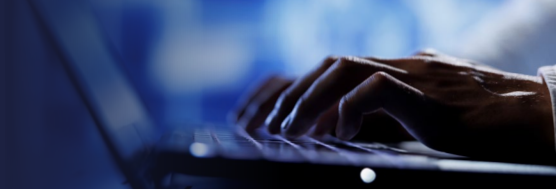
HERZOG

HERZOG FOX & NEEMAN

The UK Online Safety Act

Herzog's Practical Playbook

February 2026



INTRODUCTION

The UK Online Safety Act 2023 **("OSA")** establishes a comprehensive statutory framework governing the safety obligations of online services with a connection to the United Kingdom.

The act applies not only to services established in the UK, but also to services based outside the UK, where they enable access by UK users or where their operation gives rise to a material risk of harm to users in the UK.

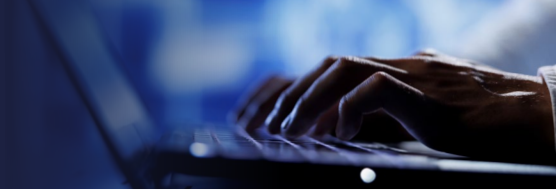
The OSA forms part of a broader **regulatory shift toward the supervision of online platforms through risk-based obligations** and ongoing regulatory oversight. Similar to recent developments in the EU, the UK regime moves away from a purely reactive enforcement model and toward a system that requires services to proactively assess, manage and mitigate risks arising from their design, functionality and user interactions. The OSA introduces legally binding duties of care, enforced by the UK watchdog **Ofcom**.

Under the OSA, **compliance is service-specific** and depends on the nature of the service, its features, its user base and the risks it presents. Providers are required to identify how **illegal content** - and, where relevant, **content harmful to children** - may arise on their services, and to implement proportionate systems and processes to address those risks.

The obligations under the OSA and its related statutory codes of practice (including the illegal content in user-to-user and search services, and the children's safety code) are ongoing in nature. Services are required to **maintain, document and periodically review** their **assessments** and **measures** as the service, its features and patterns of use evolve. Risk assessments, governance decisions, and mitigation measures must be integrated into the operation of the service and be capable of being substantiated to Ofcom upon request.

Providers are required to have regard to Ofcom's codes of practice and may comply either by following them, or by adopting alternative measures, provided they can demonstrate that those measures achieve equivalent compliance outcomes.

To assist with understanding and navigating between the various regulatory requirements and the **layered system of duties**, we are pleased to share Herzog's OSA Practical Playbook, providing explanation about its scope, key practical takeaways and insights.



SCOPE OF APPLICATION: WHO AND WHAT IS REGULATED

The OSA applies to the following **regulated online services**[1] including:

User-to-User services
services that enable users to generate, upload, or share content with other users

Search services
services that include a search engine or search functionality

Each service must be assessed separately.

A service may fall within scope where it:

- Has a significant number of UK users
- Targets the UK market, or
- Presents a material risk of harm to users in the UK

The place of incorporation of the provider is not determinative.

[1] Referred to in the legislation as "part 3 services".
The act also includes regulatory duties for providers of pornographic content, which are outside the scope of this document.

STRUCTURE OF DUTIES

The OSA establishes a layered system of duties. Certain obligations apply to all regulated services, while others are triggered based on risk and access assessments.

Illegal Content Duties - All Regulated Services

All regulated services must:

Carry out and maintain an **illegal content risk assessment**. The assessment covers the risk that:

- Users may encounter illegal content
- The service may be used to facilitate criminal activity

Assessments should identify relevant harms, evaluate likelihood and severity and document the rationale for selected mitigation measures. Ofcom has published an Illegal Content Risk Assessment template, which provides a widely accepted baseline structure.

Implement proportionate measures to prevent users from encountering illegal content and to minimize its duration and dissemination.

Maintain effective reporting, moderation and removal processes.

Keep written records of assessments, decisions and reviews, and make them available to Ofcom upon request.

Review and update assessments - at least annually or after a significant change to the service.

STRUCTURE OF DUTIES

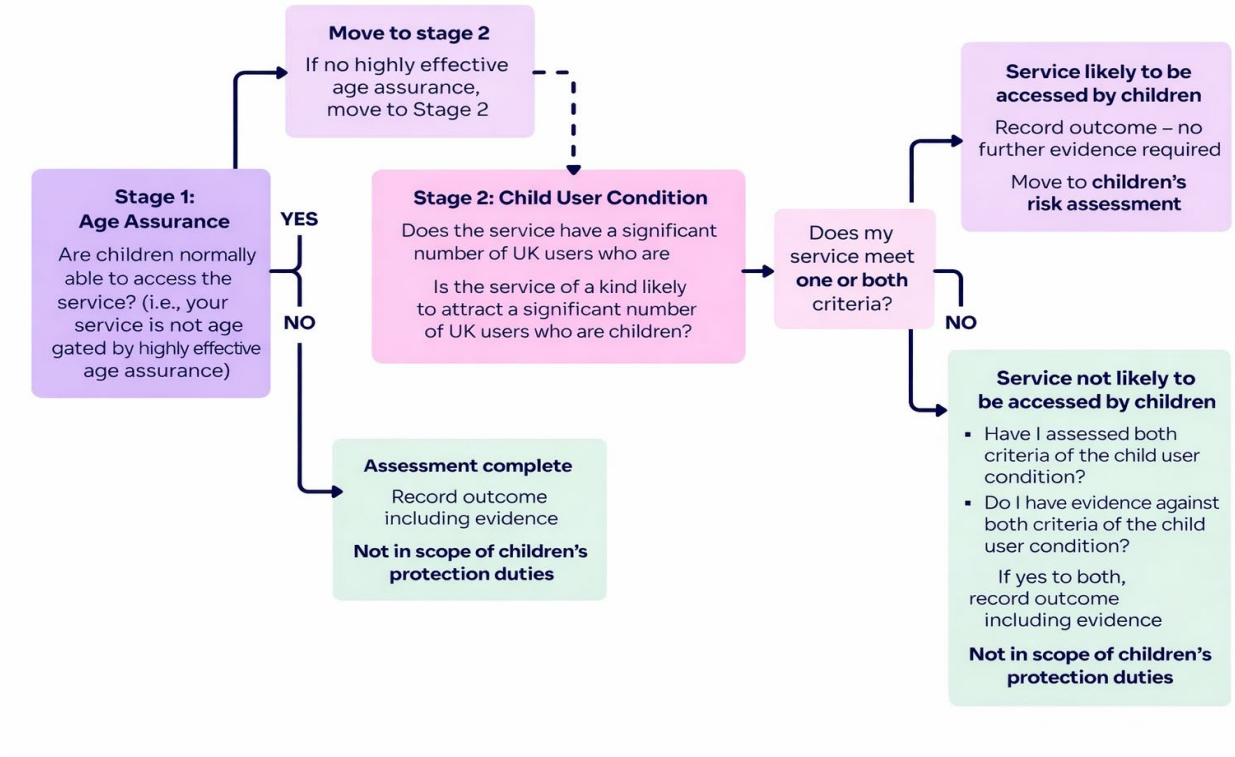
Children's Safety Duties - Gateway Structure

Children's safety duties apply automatically where children are likely to access the service. The key threshold decision is made through a children's access assessment.

1. Children's access assessment

Providers must assess **whether children (under 18) are likely to be able to access the service or any part of it**. The conclusion that children cannot access the service is defensible **only** where:

- Highly effective age assurance measures are in place; or
- The child-user condition is not met (i.e. the service doesn't have a significant number of UK users, and is not of a kind likely to attract children)



Currently, Ofcom has not published a standardized template for this access assessment, so it would have to be based on a format tailored to the relevant service.

STRUCTURE OF DUTIES

Children's Safety Duties - Gateway Structure

2. Following a positive assessment

If children **are likely to access the service, the full children's safety regime applies**. In such a case, providers must:

Carry out and maintain a **children's risk assessment** that:

- Considers different age groups
- Evaluates how service features and content types create risk
- Assesses likelihood and severity of harm
- Identifies proportionate, age-appropriate mitigation measures

Ofcom has a template for Children's Risk Assessments that is useful to follow.

Implement proportionate and age appropriate **measures to protect children** from harmful content.

Maintain **systems and processes** for:

- **Restricting** children's access, where applicable
- **Reporting** harmful content; and
- **Swift** removal where it appears

Keep written records of assessments, decisions and **reviews**. Records should be retained and made available to Ofcom upon request.

Review and update assessments - at least annually or after significant service changes.

Ofcom provides an interactive digital tool to help services understand which duties apply and to structure their risk assessment processes. Use of the tool does not remove responsibility for compliance but can support internal assessment and documentation.

Women and Girls

Risk assessments should consider how certain harms may disproportionately affect women and girls, including risks relating to sexual exploitation, harassment, coercive behavior, image-based abuse, and grooming as informed by the Ofcom Guidance on Online Safety for Women and Girls. These considerations are particularly relevant for services that enable social interaction or messaging, or content sharing.

COMPLIANCE MEASURES

Ofcom codes of practice set out **recommended compliance measures**. These include:

- **Content moderation** systems
- **Reporting** and **complaints** mechanisms
- **User controls** and safeguards
- **Age assurance** and access controls
- Internal **escalation**, **monitoring** and **governance** processes

Providers adopting alternative measures must be able to demonstrate that those measures achieve equivalent compliance outcomes.

Enforcement and Sanctions

Ofcom is vested with broad investigative and enforcement powers, including the authority to require the provision of information, direct changes to systems and processes, and impose financial penalties.

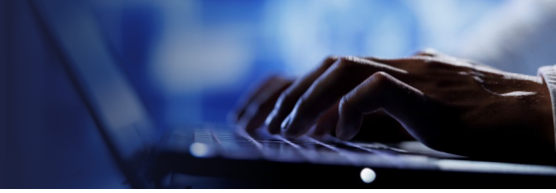
Monetary sanctions may reach the higher of £18 million or 10% of a provider's global annual turnover. In cases of serious or persistent non-compliance, Ofcom may also impose business disruption measures, including restrictions on access to the services in the UK.

Ofcom has confirmed that the regime is fully operational and that **enforcement activity is underway**, with a particular focus on the adequacy, governance and evidencing of risk assessments.

Conclusion

The Online Safety Act represents a **fundamental shift in how online services are regulated**. Compliance is no longer assessed solely by reference to policies or legal terms on paper, but by the quality of a service's risk assessments, governance and ability to **evidence decisions in practice**.

Early, structured engagement with the regime is key to reducing regulatory risk and maintaining operational flexibility as enforcement activity accelerates.



HERZOG'S TECHNOLOGY REGULATION DEPARTMENT

Herzog's Technology Regulation Department is a recognized market leader in its field.

The team is led by domain experts who possess a unique set of vital, **interdisciplinary** and **global** regulatory advisory skills, and are uniquely positioned to advise a range of clients, including leading multinational technology companies as well as start-ups and disruptive technologies vendors, on applicable regulatory and compliance considerations in numerous technological areas.

We understand that the **regulatory exposure** and scope of required **attention** of almost any company operating in the **digital and technological sphere** are much wider than one specific jurisdiction or legal discipline. As our clients are often on the forefront of this ever-evolving landscape, we further understand the impact of industry trends and compliance demands on our clients' businesses. Therefore, our team possesses in-depth knowledge of the increasing volume of regulations, enforcement actions, legislative and industry trends in a **myriad of jurisdictions, digital platforms** and leading **self-regulatory** guidelines. This enables our team to offer **practical**, **holistic** and **comprehensive** solutions for complex situations often presented by innovative technologies and disruptive business solutions, providing "hands-on" support to our clients on the strategic, corporate and operational aspects of their business, with the aim of mitigating our clients' legal and business risks.

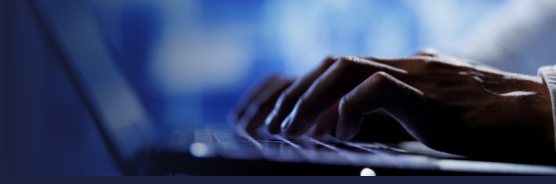
eCommerce, digital advertising, content and marketing have all become integral to almost every company's business model these days. Advising on these matters requires a high degree of know-how and expertise in order to navigate interdisciplinary and often conflicting requirements of the law, platforms' rules and guidelines, along with technological considerations and our clients' commercial needs.

We advise clients across the full lifecycle of Online Safety Act compliance, from initial scoping and risk classification through to operational implementation and regulatory engagement. Our support includes:

- Assessing whether, and to what extent, services fall within the scope of the OSA and identifying the applicable statutory duties;
- Designing, structuring, and documenting illegal content and children's risk assessments in line with Ofcom's expectations;
- Advising on children's access assessments, age-assurance strategies and associated governance considerations;
- Mapping service features, functionalities and user journeys against Ofcom's Codes of Practice;
- Developing proportionate, risk-based and defensible compliance frameworks that are operationally workable and regulator-ready;
- Supporting engagement with Ofcom, including responses to information requests, supervisory inquiries, and enforcement-related correspondence.

HERZOG
HERZOG FOX & NEEMAN

The UK Online Safety Act



Ariel Yosefi | Partner
Head of Technology Regulation
yosefia@herzoglaw.co.il

Dan Shalev | Partner
Technology Regulation
shalevd@herzoglaw.co.il

Eden Lang | Partner
Technology Regulation
lange@herzoglaw.co.il

Or Noy | Partner
Technology Regulation
noyo@herzoglaw.co.il

On Dvori | Associate
Technology Regulation
dvorio@herzoglaw.co.il

Zohar Malul | Associate
Technology Regulation
malulz@herzoglaw.co.il

Omri Bar On | Associate
Technology Regulation
barono@herzoglaw.co.il

Adaya Ziv-Kisos | Associate
Technology Regulation
Zivkisosa@herzoglaw.co.il

Eden Lapid | Associate
Technology Regulation
lapide@herzoglaw.co.il

Yoel Toledano | Associate
Technology Regulation
toledanoyo@herzoglaw.co.il

Elias Shehadeh | Intern
Technology Regulation
shehadehe@herzoglaw.co.il

Tamara Mascisch Cohen | Visiting Intern
Technology Regulation
cohentam@herzoglaw.co.il

Noya Schwartz | Law Student
Technology Regulation
schwartzn@herzoglaw.co.il

Ido Manor | Partner
Technology Regulation
manori@herzoglaw.co.il

Ruly Ber | Partner
Technology Regulation
berr@herzoglaw.co.il

Dima Zalyalyeyev | Partner
Technology Regulation
zalyalyeyevd@herzoglaw.co.il

Kevin David Gampel | Associate
Technology Regulation
gampelk@herzoglaw.co.il

Tal Habas | Associate
Technology Regulation
habast@herzoglaw.co.il

Yonatan Glatt | Associate
Technology Regulation
glatty@herzoglaw.co.il

Liron Adar | Associate
Technology Regulation
adarl@herzoglaw.co.il

Kobi Plotkin | Associate
Technology Regulation
plotkiny@herzoglaw.co.il

Yuval Glazer | Associate
Technology Regulation
glazery@herzoglaw.co.il

Gal Mechtinger | Associate
Technology Regulation
mechtingerg@herzoglaw.co.il

Elad Rozenvasser | Intern
Technology Regulation
rozenvassere@herzoglaw.co.il

Korin Arbel | Pre-Intern
Technology Regulation
arbelk@herzoglaw.co.il