UK Online Safety Act: Overview

TaylorWessing

Purpose

The Online Safety Act (OSA) introduces a new regulatory regime to protect users from harm online resulting from user-generated content (UGC). The regime will focus on processes and systems rather than the removal of specific pieces of content.

Obligations on service providers caught will include (a) duties to conduct **risk assessments**, (b) various **safety duties**, (c) **transparency, reporting and redress duties**, (d) duties to protect certain types of **content/ rights** and (e) various **other duties** eg around fraudulent advertising.

Services within scope

(Part 2)

The OSA applies to providers of:

(a) User-to-user services – internet services which allow content generated, uploaded or shared by a user to be encountered by another user(s).

(b) Search services – internet services that allow users to search more than one website or database.

(c) Pornographic content services – not covered in this document.

An **internet service** includes anything made available by means of the internet or a combination of the internet and an electronic communications service. Websites, apps and other software are covered, as are public and private channels.

Content means anything that can be communicated by means of an internet service, whether publicly or privately (and includes content automatically generated by AI/bots). References to content in this table largely mean regulated UGC.

	All user-to-user services and search services	**Category 1 services** (and Category 2 services, where indicated)	**User-to-user services and search services likely to be accessed by children**
Service providers caught by the OSA	Search engines, content-sharing platforms, social media platforms, online marketplaces, online gaming services, blogs, forums etc which meet the definition of a user-to-user service or search service and are otherwise within scope. *Note that the duties below are set out in relation to user-to-user services; similar duties apply to search services.*	Category 1 services are user-to-user services that meet threshold conditions to be set out in secondary legislation relating to the number of users, service functionality and/or other factors (section 95). *We consider Category 1 is primarily intended to apply to the largest social media or video-sharing services, given policymakers' focus on content virality, frictionless sharing, and endless automatic serving of interest-based content as potential sources of harm.* *Note that the OSA also introduces the concept of Category 2A and 2B services, which are search services and user-to-user services respectively that meet certain threshold conditions to be set out in secondary legislation (section 95).* *The below obligations relate to Category 1 services only unless otherwise indicated.*	Services are likely to be accessed by children (under-18s) where the children's access assessment concludes that: (a) it is possible for children to access the service or a part of it (b) there is a significant number of children who are users of the service/part of the service, or the service/part of the service is of a kind likely to attract a significant number of users who are children ((b) being the child user condition) (section 37). Duties relate only to the parts of a service possible for children to access. A provider is only entitled to conclude that children are not able to access the service/part if age verification/estimation (but not self-declaration of age) is used with the result that children are not normally able to access that service/part. Services that fail to carry out the assessment will be considered likely to be accessed by children, and OFCOM can determine that a service is likely to be accessed by children in certain circumstances.
Definitions	Many of the obligations apply to illegal content and priority illegal content. **Illegal content** (section 59) comprises content that amounts to: **(a) A priority offence** (terrorism offences, CSEA offences and other priority offences specified in Schedule 7). **(b) Any other offence of which the victim is an individual(s).** Offences concerning IP infringement, safety/quality of goods, performance of a service by unqualified person and offences under The CPUT Regs are excluded. **Priority illegal content** effectively means content that amounts to a priority offence. Part 11 deals with how providers are to make judgements about whether content falls within relevant definitions. No account is to be taken of whether or not anything done takes place in the UK in determining whether content amounts to an offence. Note that the OSA will create various new criminal offences, including offences of encouraging or assisting serious self-harm, sharing or threatening to share intimate photos/films, sending/showing flashing images and various communications offences (Part 10).	Many of the obligations apply to **adult user content** (content which encourages/promotes/instructs on suicide, deliberate self-injury or eating disorders/ behaviours or content which is abusive (and targets race, religion, sex, sexual orientation, disability or gender reassignment) or incites hatred against people based on these characteristics (new section 16)).	Many of the obligations apply to content of different types that is harmful to children. **Content that is harmful to children** (section 60) means: **(a) Primary priority content that is harmful to children** (pornographic content or content that encourages/ promotes/instructs on suicide, deliberate self-injury or eating disorders/behaviours). **(b) Priority content that is harmful to children** (bullying content or content which (a) is abusive and targets race, religion, sex, sexual orientation, disability or gender reassignment (b) incites hatred against people based on these characteristics, (c) encourages/ promotes/instructs on serious violence against a person or a challenge/stunt likely to result in serious injury, (d) depicts serious violence or (in graphic detail) serious injury against a person/ animal/fictional creature, (e) encourages self-administration of physically harmful substances). **(c) Content not within (a) or (b) that presents a material risk of serious harm to an appreciable number of children in the UK (non-designated content that is harmful to children).** Part 11 deals with how providers are to make judgments about whether content falls within relevant definitions. References to harm include cumulative harm (section 234).
Risk assessments duties	■ **Carry out an illegal content risk assessment** (section 9). Assessments must be kept up to date/repeated, including when OFCOM makes any significant changes to risk profiles or there is a significant change to any aspect of the service's design or operation.	■ **Carry out an adult user empowerment risk assessment relating to adult user content** (new section 14). Similar obligations as for the illegal content risk assessment.	**Carry out a children's risk assessment** (section 11). Similar conditions as for the illegal content risk assessment. OFCOM must also be notified of any non-designated content harmful to children identified in the assessment.

UK Online Safety Act: Overview

TaylorWessing

Encountered includes reading, viewing, hearing or otherwise experiencing.

For **search services**, the duties imposed only apply to UGC that may be encountered in or via search results (including by clicking on them), not UGC encountered from subsequent interactions with internet services other than the search service.

Providers are defined in section 226.

There is potential for powers to be introduced to regulate app stores (section 215).

While many obligations relate to all user-to-user and search services, there are additional obligations on category 1 and 2 services and services likely to be assessed by children. These are reflected in the columns of this table.

Territory

(Section 4)

The OSA applies to services which have **links to the UK**. A service has links to the UK if: (a) it has a significant number of UK users, or (b) UK users form one/the target market for the service or (c) it is capable of being used in the UK and there are reasonable grounds to believe the UGC/search content on the service presents a material risk of significant harm to individuals in the UK.

Exempt services

(Section 4 and Schedule 1)

The following services are **exempt:**

(a) User-to-user services that only enable UGC in the form of (i) emails, (ii) SMS messages, (iii) MMS messages and/or (iv) one-to-one live aural communications, and (v) related identifying content (eg a username).

	All user-to-user services and search services	Category 1 services (and Category 2 services, where indicated)	User-to-user services and search services likely to be accessed by children
Risk assessments duties	■ **Carry out a children's access assessment** (section 35 & 36). This will determine whether children are able to access the service and the child user condition is met - see the "user-to-user services and search services likely to be accessed by children" column in this table. Assessments must be repeated regularly and on the happening of certain events.		
Safety duties	**Illegal content** (section 10). ■ Take or use proportionate measures relating to the design or operation of the service to (a) prevent individuals from encountering priority illegal content, (b) effectively mitigate and manage the risk of the service being used for the commission or facilitation of a priority offence and (c) effectively mitigate and manage the risk of harm (from illegal content) to individuals ((b) and (c) as identified in the risk assessment). ■ Use proportionate systems and processes to (a) minimise the length of time priority illegal content is present and (b) swiftly take down any illegal content when alerted/aware. ■ Specify in T&Cs how individuals are to be protected from illegal content including any proactive technology used; ensure these provisions are clear and accessible in T&Cs; apply T&Cs consistently; summarise findings of most recent illegal content risk assessment in T&Cs. ■ While not completely clear, the obligation to "prevent" individuals encountering priority illegal content does not seem to require the use of proactive technology (although see sections 121 and 136 about OFCOM's powers to issue notices requiring use/development of accredited technology re terrorism and CSEA content and to issue confirmation decisions requiring the use of proactive technology).	**Empowering adult users** (section 15). ■ Include proportionate features to allow adult users to reduce the likelihood of the user encountering - or alert the user to - adult user content (control features). ■ Control features to be available to all adult users, easy to access and details to be included in T&Cs. ■ Ensure that all registered adult users are asked at the earliest opportunity which control features are to be applied. ■ Include features allowing adult users to filter out non-verified users. ■ Summarise findings of most recent adult user empowerment risk assessment in T&Cs.	**Protecting children** (section 12). ■ Take or use proportionate measures relating to the design or operation of the service to effectively mitigate and manage the risks (and impact) of harm to children in different age groups (as identified in the risk assessment). ■ Use proportionate systems and processes to operate the service to (a) prevent children from encountering primary priority content that is harmful to children and (b) protect children in age groups judged to be at risk of harm from encountering other content that is harmful to children. ■ The duty to "prevent" children encountering primary priority content harmful to children requires providers to use age verification/estimation (unless T&Cs indicate such content is prohibited and the policy applies to all users). Even where not required, age verification and estimation are given as examples of what can be used to comply with all above obligations. ■ Specify in T&Cs how the above and related protections are to be achieved including any proactive technology used; ensure these provisions are clear and accessible in T&Cs, apply T&Cs consistently; and summarise the findings of most recent children's risk assessment in T&Cs.
Transparency, reporting and redress duties	■ **Content reporting** (section 20). Use systems and processes that allow easy reporting of illegal content. ■ **Complaints procedures** (section 21). Operate an easy to access/use complaints procedure (also contained in T&Cs) that allows for complaints about illegal content, compliance by services with safety and other duties, take downs, user sanctions and use of proactive technology. ■ **Record-keeping and review** (section 23). Keep records of risk assessments (including how carried out and findings) and supply copy to OFCOM. Keep records of measures taken to comply with duties and reasons for using methods not in codes of practice. Review compliance with duties regularly and after making significant changes to any aspects of the service's design or operation. ■ **Information re investigation into death of a child** (after section 101). Various powers for OFCOM to require information about use of a service by a child on request of eg a coroner.	■ **Complaints procedures** (section 21). Operate an easy to access/use complaints procedure which allows complaints about compliance with Category 1 safety and other duties. ■ **T&Cs** (sections 71 and 72). Not act against users except in accordance with T&Cs and various other duties about T&Cs with various exceptions. ■ **Annual transparency reporting** (section 77). (also applies to Category 2 services). ■ **Record-keeping and review** (section 23). Keep records of adult user empowerment risk assessment (including how carried out and findings) and supply copy to OFCOM. ■ **Deceased child users** Obligation to specify approach in T&Cs and to comply with those T&Cs (also applies to Category 2A and 2B services (section 75)).	■ **Content reporting** (section 20). Use systems and processes that allow easy reporting of content that is harmful to children present on the service where possible for children to access such content. ■ **Complaints procedures** (section 21). Operate an easy to access/use complaints procedure that allows for complaints about content that is harmful to children, compliance by services with children's safety duties, take downs, user sanctions and incorrect age assessments. ■ **Record-keeping and review** (section 23). Keep records of risk assessments (including how carried out and findings) and supply copy to OFCOM. Keep records of measures taken to comply with duties and reasons for using methods not in codes of practice. Review compliance with duties regularly and after making significant changes to any aspects of the service's design or operation.

UK Online Safety Act: Overview

TaylorWessing

(b) Limited functionality services – user-to-user services that only allow users to communicate by (i) posting/sharing comments or reviews relating to content published by or on behalf of the service provider, (ii) applying likes/dislikes, emojis/symbols, yes/no voting or rating/scoring such content, comments or reviews, or (iii) displaying identifying content in relation to such activities.

(c) Internal business resources – user-to-user or search services comprising internal resources or tools provided by a business and available only to a closed group of people connected to the business.

(d) User-to-user services or search services provided by public bodies or by providers of education or childcare – in the exercise of their public functions, or for the purposes of that education or childcare.

There are similar exemptions for parts of services and content of the above kinds (sections 5 and chapter 7).

There are transitional provisions for video-sharing platform services (Schedule 17).

Section 237 summarises all definitions.

	All user-to-user services and search services	Category 1 services (and Category 2 services, where indicated)	User-to-user services and search services likely to be accessed by children
Duties to protect certain content/rights	When deciding on and implementing safety policies/procedures, have regard to the importance of protecting (a) users' right to freedom of expression within the law and (b) users from unlawful breaches of privacy (including relating to data protection) (section 22).	■ Protect content of democratic importance (section 17), news publisher content (section 18) and journalistic content (section 19). ■ Assess the impact of safety measures and policies on (a) freedom of expression and privacy and (b) the availability/treatment of news publisher content and journalistic content; and publish and keep such impact assessments up to date (section 23).	N/A
Other duties	■ Duties about reporting CSEA content to the NCA (section 66). ■ Various duties on certain providers of pornographic content (part 5).	■ Duties about fraudulent paid-for advertising on the service (chapter 5). (Category 2A services also have similar duties.) ■ Duties about identity verification (section 64).	N/A
Enforcement and sanctions	■ OFCOM is the regulator which will oversee the regime. It has the power to charge fees on services within scope. ■ It must produce codes of practice relating to nearly all duties, which will include how the duties can be met. Providers who take or use a measure described in a code of practice will be treated as complying with the relevant duty. Those that do not won't necessarily be deemed not to be complying. ■ It must publish guidance on various duties (including about protecting women and girls – section 54), as well as examples of the type of content it considers to fall within the definitions above. ■ OFCOM must establish and maintain a register of services including certain services that meet the Category 1, 2A and 2B threshold conditions (section 94). It must carry out various risk assessments (section 98). ■ OFCOM has the power to require information from services including the naming of senior managers (sections 100-103) and to conduct investigations, interviews inspections and audits (sections 105-108). This includes oversight of algorithms. ■ Various offences are created (eg for failure to comply with an information notice) and senior managers can be liable for some offences (sections 108-113). Parent entities can be liable for failures of subsidiaries and vice versa; fellow subsidiaries can also be liable, as can controlling individuals (section 197 and Schedule 15). ■ OFCOM has various enforcement powers (sections 130-151), including to issue fines of up to 10% of annual global turnover or £18m (whichever greater) (Schedule 13) and to obtain various business disruption measures. ■ There are various provisions about appeals against OFCOM decisions and super-complaints (Part 8).		

Our team

Mark Owen
Partner
+44 20 7300 4884
m.owen@taylorwessing.com

Xuyang Zhu
Senior Counsel
+44 20 7300 7000
x.zhu@taylorwessing.com

Timothy Pinto
Senior Counsel
+44 20 7300 7000
t.pinto@taylorwessing.com

Louise Popple
Senior Counsel
+44 20 7300 4787
l.popple@taylorwessing.com

Debbie Heywood
Senior Counsel
+44 20 7300 7000
d.heywood@taylorwessing.com

Our locations

2000+ people
1100+ lawyers
300+ partners
29 offices
17 jurisdictions

Austria	Klagenfurt | Vienna
Belgium	Brussels
China	Beijing | Hong Kong | Shanghai
Czech Republic	Brno | Prague
France	Paris
Germany	Berlin | Düsseldorf | Frankfurt | Hamburg | Munich
Hungary	Budapest
Netherlands	Amsterdam | Eindhoven
Poland	Warsaw
Republic of Ireland	Dublin
Slovakia	Bratislava
South Korea	Seoul*
UAE	Dubai
Ukraine	Kyiv
United Kingdom	Cambridge | Liverpool | London | London TechFocus
USA	New York | Silicon Valley

* In association with DR & AJU LLC