Cooley

The Online Safety Act: Child Access Duties for the Gaming Industry

April 9, 2025

Under the UK Online Safety Act 2023 (OSA), a wide range of online services are subject to extensive new obligations related to illegal content and content harmful to children.

The UK's Online Safety regulator, Ofcom, has now set out its children's access guidance, along with guidance on what constitutes effective age assurance. These publications triggered a requirement for all in-scope services to assess whether they are likely to be accessed by children (a child, for the purpose of this legislation, being a person in the UK under the age of 18). This children's access assessment must be completed by **16 April 2025.**

If a service is likely to be accessed by children, the service provider will be required to comply with children's protection duties – namely, carry out a children's risk assessment (guidance on this is due in April 2025) and comply with Ofcom's Protection of Children Codes (which will come into effect in July 2025).

Ofcom has previously stated that online gaming is a 'fundamental form of entertainment for children'. Therefore, gaming platforms will no doubt be a target for the regulator.

In advance of the upcoming deadline, to the extent you have not already taken action to confirm whether you are in scope of the OSA and/or carry out a children's access assessment, we set out below the key points to bear in mind.

Are you in scope of the OSA?

By way of reminder to check whether you're in scope:

Type of service

If you provide a service which allows users to interact with each other in any way, then you are likely to fall within the user-to-user service bracket and be in scope of the OSA.

Offline games are not caught by the OSA. However, online gaming platforms are likely to be caught by the OSA where they have functionalities that enable user-to-user interaction. For example, multiplayer games – be it smaller team-based games or massively multiplayer online games – which have text or voice chat functionalities will be in scope, as well as games that allow for the sharing of user-generated content (including livestreaming), or those that use virtual reality or augmented reality to create communal online spaces.

Size of service

There are no exceptions for small or micro businesses. If your service is a user-to-user service, then it is irrelevant how big or small it is, and the duties and obligations apply.

Territorial scope

This is broad. Services do not have to have a presence or operations in the UK. They do not even need to specifically target UK users. It may be enough that your service is accessible by UK users if the risks presented by the service are significant.

Children's access assessment

The children's access assessment is a two-stage test.

Stage 1

Is it possible for children to access the service (in full or part)?

- If the service has in place highly effective age assurance (HEAA), explained further below, then it is not in scope. However, as explained below, the bar for HEAA is high, and most services will not meet it.
- If the service does not have in place HEAA, then it may be in scope, depending on the outcome of Stage 2.

Stage 2

There are two questions here: Do a significant number of children access the service, and is the service likely to attract a significant number of children? Unless the answer to **both** questions is no, the service will be in scope.

- The OSA does not define what is meant by a 'significant number' of children; however, Ofcom guidance suggests that this is 'likely to depend on the nature and context of the service'. So, for example, if a relatively high percentage of the overall user base are children, this is likely to be "significant'. Equally, the guidance also notes that even a relatively small number of children could be deemed 'significant' if the risks to children presented by the service are serious.
- Factors that service providers **in the gaming space** should consider include the following:
    - Does the service provide benefits to children? If the designated age rating for the game includes those under 18, the answer to this will be yes.
    - Does the content on the service appeal to children? This can apply even where a game has an '18' rating and there are already active steps to limit children's access. If you have had reports of children wrongfully trying to play a game for adults or access a service associated with a game that is restricted to adults, this would suggest that the content is appealing to children. Gaming platforms also should be mindful that older children, e.g. late teens, may be interested in games targeted at adults.
    - Is the design of the service appealing to children? This is broad and could capture colours and presentation styles, as well as features and functionalities that appeal to children, such as the ability to make a user profile and/or make connections with others.
    - Do children form part of your commercial strategy? This could include unintentionally targeting children, e.g. if your game is advertised on other services known to be accessed by children.

The results of the children's access assessment must be documented. If you conclude that your service is not likely to be accessed by children, then you also must document your methodology and evidence for reaching this conclusion.

There is an ongoing duty to assess children's access. Services out of scope of children's protection duties are required to carry out children's access assessments regularly (and not more than one year apart).

Implementing HEAA

Ofcom has provided guidance on implementing HEAA requirements. The guidance does not prescribe how service providers can implement HEAA requirements but instead affords services a level of flexibility.

It lists the kinds of age assurance it considers to be highly effective – including photo ID matching, facial age estimation, mobile-network operator age checks, credit card checks and email-based age estimation.

It also identifies methods it does not consider highly effective – including self-declaration of age, age verification through online payment methods which do not require a user to be older than 18 (debit cards), and general contractual restrictions on the use of the service by children.

Beyond this, it sets out four criteria for assessing age assurance methods' effectiveness:

- **Technical accuracy** – the degree to which an age assurance method can correctly determine the age of a user under test lab conditions.
- **Robustness** – the degree to which an age assurance method can correctly determine the age of a user in actual deployment contexts.

- **Reliability** – the degree to which the age output from an age assurance method is reproducible and derived from trustworthy evidence.
- **Fairness** – the extent to which an age assurance method avoids or minimises bias and discriminatory outcomes.

Challenges for services can arise in implementing HEAA whilst also complying with data protection obligations. Ofcom is working closely with the UK's data protection regulator to align their guidance but tensions nevertheless remain between these two sets of regulatory requirements.

This content is provided for general informational purposes only, and your access or use of the content does not create an attorney-client relationship between you or your organization and Cooley LLP, Cooley (UK) LLP, or any other affiliated practice or entity (collectively referred to as "Cooley"). By accessing this content, you agree that the information provided does not constitute legal or other professional advice. This content is not a substitute for obtaining legal advice from a qualified attorney licensed in your jurisdiction, and you should not act or refrain from acting based on this content. This content may be changed without notice. It is not guaranteed to be complete, correct or up to date, and it may not reflect the most current legal developments. Prior results do not guarantee a similar outcome. Do not send any confidential information to Cooley, as we do not have any duty to keep any information you provide to us confidential. When advising companies, our attorney-client relationship is with the company, not with any individual. This content may have been generated with the assistance of artificial intelligence (AI) in accordance with our AI Principles, may be considered Attorney Advertising and is subject to our legal notices.

Key Contacts

Alicia Johnson-Cole London	ajohnson-cole@cooley.com +44 (0) 20 7556 4509

This information is a general description of the law; it is not intended to provide specific legal advice nor is it intended to create an attorney-client relationship with Cooley LLP. Before taking any action on this information you should seek professional counsel.

Copyright © 2023 Cooley LLP, 3175 Hanover Street, Palo Alto, CA 94304; Cooley (UK) LLP, 22 Bishopsgate, London, UK EC2N 4BQ. Permission is granted to make and redistribute, without charge, copies of this entire document provided that such copies are complete and unaltered and identify Cooley LLP as the author. All other rights reserved.