Date: 24 February 2025

This advice represents the position as at the date the advice provided. Businesses should consult relevant information and guidance on regulators' websites to keep up-to-date with the latest developments.

CASE STUDY: Ensuring Highly Effective Age Assurance on a User-to-User Service

This is an anonymised version of a query submitted to the DRCF AI and Digital Hub ('the Hub').

The query in this case study has been responded to by the following DRCF regulators ('we', 'us', 'our'):

- Office of Communications ('Ofcom'); and
- Information Commissioner's Office ('ICO').

This informal advice is provided in line with the Conditions for Participation.

Our informal advice is provided to a business based on our current understanding of the legal and regulatory frameworks within our remits and how they apply to the business's service. This informal advice should not be treated as an exhaustive account of the issues linked to a business's service or represent an endorsement of their proposed innovation.

Our informal advice is specific to a business's circumstances as described by them in the information they provided to the Hub.

Our informal advice is provided without prejudice to any future regulatory intervention by any DRCF or non-DRCF regulator and is not a substitute for independent legal advice which a business may wish to seek in advance of the launch of their service.

It is ultimately a business's responsibility to assess their position under the law and regulatory regime, with the benefit of independent legal advice as necessary. Recognising that some regulatory regimes are still developing and could change over time, businesses have a responsibility to keep up to date with the latest position.

A non-confidential version of the informal advice provided to the applicant is attached to this case study. This informal advice was provided on 24 February 2025 and represents the position as at 24 February 2025. Businesses should consult relevant information and guidance on regulators' websites to keep up to date with the latest developments.

Summary of Query and Response

Business F is building a platform where adult users can share intimate images safely. Business F's service is designed for users aged 18 and over and should not be accessed by children.

Business F's question was:

Our service is designed for users aged 18 and over and should not be accessed by children. What do we need to do to ensure we are using a highly effective form of age assurance?

- The response highlights key expectations and duties for user-to-user services under the Online Safety Act, especially services likely to be accessed children and particularly those with content that is harmful to children. For some user-to-user services, this includes a duty to protect them from harmful content by deploying highly effective age assurance.
- Ofcom defines age assurance and set out how business F can implement highly effective age assurance and the types of age assurance capable of being highly effective and those which are not.
- Ofcom outlines how business F's process as a whole must be highly effective and fulfill the necessary four criteria of technical accuracy, robustness, reliability, and fairness as well as considering two additional principles of accessibility and interoperability.
- The ICO sets out how age assurance methods deployed by business F must also be compliant with data protection law, and recommend business F complete a DPIA justifying their age assurance approach and the level of certainty it provides in determining a user is 18+.

Introduction to the regulators

The query has been responded to by the ICO and Ofcom. A brief introduction to each regulator has been included below.

Each regulator is responsible for separate legal regimes with different requirements that may be applicable to the same set of facts, and it will be necessary to take steps to comply with each regime as set out.

Ofcom

Ofcom is the regulator for the communications services that we use and rely on each day. Ofcom regulates the TV and radio sectors, fixed line telecoms, mobile, postal services, plus the airwaves over which wireless devices operate. Since 2023, Ofcom is the UK regulator for online safety. Ofcom oversees the following laws which are relevant to this informal advice:

- Online Safety Act 2023 ('OSA')

Under the **OSA**, Ofcom's mission is to make life safer online in the UK, especially for children, by ensuring services have appropriate systems and processes to protect people from harm. The Online Safety regime is now in force and Ofcom published its first codes of practice and guidance on protecting people from illegal harms online in December 2024. For a comprehensive overview of the OSA and Ofcom's roadmap to regulation, please see here.

Online services need to determine whether they are in scope of the OSA, and bring themselves into compliance if they are. Under the OSA there are three categories of services that will be legally responsible for keeping people, especially children, safe online. This includes:

- **User-to-user (U2U) services,** where people can create and share content (e.g. images, videos, messages or comments), or interact with each other;
- **Search services,** where people can search more than one website and/or database; and
- **Pornography services,** where an individual or a business publishes or displays pornographic content.

ICO

The Information Commissioner's Office ('ICO') is the UK's independent public authority set up to uphold information rights. The ICO oversees the **UK General Data Protection**

Regulation (UK GDPR) and developed the Age Appropriate Design Code ('AADC'), also known as the **Children's Code**. The Code sets out 15 standards that online services must follow to ensure they protect children's privacy, covering areas such as data minimisation, default privacy settings, and age assurance. It applies to services **likely to be accessed by children**, even if they are not specifically designed for them.

Under the **UK GDPR**, organisations like business F must consider data protection and privacy issues upfront. The informal advice that follows highlights some key data protection considerations for business F's intended processing activities.

Regulator Response References

In the table below, we set out the relevant regulator and the respective responses that they have input on. Each regulator is only responsible for the responses within their regulatory remit as noted in this table.

Regulator	Relevant Responses
Ofcom	1.1 – 1.26 1.35 – 1.39 1.41
ICO	1.27 – 1.34 1.40 – 1.41

Response

Online Safety

1.1. Business F's service provides a platform to consensually share intimate images between adults and that it is not designed to be used by children.

1.2. Based on Ofcom's understanding of the features of business F's platform from the information they provided in their application, their product is likely to fall under Part 3 of the OSA as a **U2U service.** This is because:

- the service enables users to interact with one another, including by generating, uploading or sharing content, such as images, videos, messages or comments, with other users of the service; and
- the service intends to have links with the UK:
    - by having either a significant number of UK users or the UK being a target market for the service as per section 4(5) of the OSA; or
    - by being capable of being used in the United Kingdom by individuals, and there are reasonable grounds to believe that there is a material risk of significant harm to individuals in the United Kingdom presented by user-generated content present on the service as per section 4(6) of the OSA.

1.3. For the purposes of this informal advice, Ofcom has **not considered** business F's platform to constitute a Part 5 service[1] because it does not contain pornographic content which is published or displayed on the service by the provider.

1.4. Ofcom recommends using the dedicated Online Safety Regulation Checker tool which can help determine whether a service could be considered a 'pornography service' in addition to or instead of being a U2U service.

1.5. For ongoing questions about the application of the OSA, Ofcom has a website page here where companies can submit queries or they may wish to contact Ofcom's online safety team directly at OSengagement@ofcom.org.uk.

Expectations of a U2U Service: protecting children

[1] An online service falls within Part 5 of the OSA if it publishes or displays so called regulated pornographic content. If the content in question falls within the definition of pornographic content (in the Act) it is then necessary to consider if the pornographic content is published or displayed by the provider of the online service or someone acting on their behalf. Ofcom provides further guidance on what is meant by published or displayed in the Part 5 guidance

1.6. Securing a higher level of protection online for children is one of the key objectives of the OSA. The OSA places specific duties on U2U services that are likely to be accessed by children, which includes using proportionate systems and processes to prevent children from encountering 'primary priority content' that is harmful to children.

1.7. The OSA defines primary priority content that is harmful to children as including pornographic content (which is defined as content of such a nature that it is reasonable to assume that it was produced solely or principally for the purpose of sexual arousal[2]).

1.8. Based on Ofcom's understanding, business F's service is designed to allow adult users to share intimate images, which Ofcom has assumed would be likely to fall within the category of pornographic content.

1.9. Ofcom has treated business F as a Part 3 U2U service, therefore this informal advice is in accordance with this type of service. However, it remains the responsibility of business F to verify whether they are classified as a Part 3 service and/or a Part 5 service.

Determining whether a service is likely to be accessed by children

1.10. The next step would be for business F to determine if their service is within scope of the child safety duties. To do this, business F will need to understand if their service is likely to be accessed by children and carry out a **children's access assessment.**

1.11. However, as noted in Ofcom's recent Statement: Age Assurance and Children's Access, business F may conclude that they are not likely to be accessed by children if they are using highly effective age assurance with the result that children are not normally able to access the service.

1.12. Ofcom understands it is business F's intention to age-gate their service such that children cannot access it.

1.13. However, if business F does not deploy highly effective age assurance to achieve this, they will need to consider whether their service is 'likely to be accessed by children'[3] as defined in in the OSA.[4] If it is, business F will need to carry out a

[2] Section 236, OSA
[3] As set out in Ofcom's Statement on Age Assurance and Children's Access, Ofcom expects that most U2U services will need to conclude that they are 'likely to be accessed by children' and so Ofcom would expect a service to have good evidence to substantiate any finding that it is not likely to be accessed by children.
[4] S.37 OSA. See also Ofcom's Children's access assessments Guidance

children's risk assessment and comply with children's safety duties.

1.14. In April 2025, Ofcom will publish the Protection of Children Codes and children's risk assessment guidance. This will mean that services likely to be accessed by children will need to conduct a children's risk assessment within 3 months (by July 2025).

1.15. Following this, services must implement measures to protect children using their services to address the risks of harms identified, such as the measures set out in the Protection of Children Codes. These measures may include introducing age checks to determine which of their users are under 18 and protecting them from harmful content.

Age Assurance

1.16. Services that do not prohibit pornography (or other types of primary priority content) are required to use highly effective age assurance to prevent children from accessing that content, which could mean preventing children from accessing the entire service.

1.17. An age assurance method refers to the particular system or technology that underpins an age assurance process. An age assurance process refers to a system or process designed to determine whether a particular user is, or is not, a child. This process is comprised of one or more age assurance methods. The effectiveness of an age assurance method will depend on how it is implemented, including whether by itself or in combination with other methods.

- Ofcom has produced dedicated guidance for Part 3[5] services to assist them in implementing 'highly effective age assurance'. Part 3 services should consult the Part 3 HEAA Guidance, as well as Section 3 of the statement, to understand Ofcom's recommendations, including further technical detail to help services implement highly effective age assurance.

Examples of Highly Effective Age Assurance

1.18. Ofcom's guidance sets out a non-exhaustive list of kinds of age assurance that we consider capable of being highly effective at correctly determining whether or not a

[5] Ofcom also has dedicated guidance for Part 5 providers. Part 5 providers should refer to this , as well as Section 3 and 4 of the Age Assurance and Children's Access statement, to understand the scope of Part 5 and how they can meet all the requirements of the Part 5 of the Act.

user is a child.

1.19. These include:

- **Open banking**: This works by, with the user's consent, accessing the information their bank has on record about the user's age and confirming whether or not the user is over 18. The user's date of birth and any other information is not shared with the relying party.
- **Photo-identification (photo-ID) matching**: This works by comparing an uploaded photo ID to an image of the user taken when the ID is uploaded to verify they are the same person.
- **Facial age estimation:** This works by analysing facial features to estimate the user's age.
- **Mobile-network operator (MNO) age checks:** Every UK MNO automatically applies a content restriction filter (CRF) to prevent children from accessing age restricted content over their mobile service. A user can remove the CRF via an age check that proves they are an adult. An MNO age check relies on checking whether the CRF is removed. If the CRF has been removed, this indicates the user is over 18. Confirmation of whether or not the user is over 18 is then shared with the relying party.
- **Credit card checks:** In the UK, individuals must be at least 18 to obtain a credit card and therefore, credit card issuers must verify the applicants age before issuing them. Credit card-based age verification works by the user entering their credit card details, after which a payment processor requests validation from the issuing bank. Approval from the issuing bank serves as proof that the user is over 18.
- **Email-based age estimation:** These solutions work by estimating a user's age based on other online services where the email address has been used. This may include instances where the email address is associated with financial institutions such as mortgage lenders.
- **Digital Identity services:** A digital identity service is a digital representation of a person that allows them to prove their identity during online and in person interactions and transactions. Reusable digital identities can be used multiple

times for various interactions and transactions. This includes digital identity wallets, which allow users to verify and store their attributes (including age) in a digital format. Verification can occur through various methods, including those mentioned above. Once verified and stored in the wallet users can choose to share specific attributes such as age or status as an adult, with a relying party.

1.20. Types of age assurance that are not capable of being highly effective include:

- **Self-declaration of age:** The OSA states that measures which require users to self-declare their age (without other methods) cannot be regarded as age assurance. These methods include: asking a user to input their date of birth without further proof to confirm this information or asking a user to tick a box confirming they are 18 or older.
- **Age verification through online payment methods which do not require a user to be over 18:** For example, verifying their age through debit cards or other cards where the card holder is not required to be 18.
- **General contractual restrictions on the user of the regulated service by children:** For example:
    - Including as part of the terms of service a condition that prohibits users under 18 years old from using the service, without any additional age assurance;
    - General disclaimers asserting that all users should be 18 years of age or older; or
    - Warnings on specific content that the content is only suitable for over 18s.

Implementing 'Highly Effective' Age Assurance

1.21. Ofcom recognises that age assurance methods are developing at pace and the list of example methods may expand over time.

1.22. Further, it is for the service provider to determine which age assurance method(s) to use in order to implement an age assurance process that is appropriate to meet its duties under the Act. Implementing one of the example methods is not a guarantee that the service is acting in accordance with the OSA. Service providers must be able to demonstrate that the method has (or methods have) been implemented in

such a way that **ensure the overall process as a whole is highly effective**.

1.23. To ensure that an age assurance process is, in practice, highly effective at correctly determining whether or not a user is a child, business F should ensure that the process fulfils each of the following four criteria:

- **Technical accuracy:** the degree to which the age assurance method can correctly determine the age of a user under 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

1.24. Ofcom's Part 3 HEAA Guidance provides further detail on how to assess each of these criteria:

- Ofcom recognises that different kinds of age assurance – or even the same kinds of age assurance provided by different companies – may perform more strongly in some of these criteria than others. Business F should have regard that their age assurance method(s) as a whole fulfils each of the criteria.
- As well as meeting the four criteria, business F's method should be easy to use and work for all users. Failing to do so might unduly prevent adult users from accessing legal content. Business F should consider the following two principles:
    - **Accessibility:** the principle that age assurance should be easy to use and work for all users, regardless of their characteristics or whether they are members of a certain group.
    - **Interoperability:** the ability for technological systems to communicate with each other using common and standardised formats.

1.25. It may be possible for children to circumvent the age assurance process or access control mechanisms a provider has put in place. These risks can be mitigated by service providers ensuring their age assurance process is appropriately robust. Business F should identify and take appropriate steps to mitigate against methods of circumvention that are easily accessible to children, and where it is reasonable to

assume children may use them.

1.26. Finally, all age assurance methods involve the processing of personal data and should follow a **data protection by design approach**. Ofcom and the ICO have worked closely to adopt a cohesive approach supporting compliance with our respective regulatory regimes. Both regulators agree that compliance with both the online safety and data protection regime is mandatory and should not be considered a trade-off. The joint guidance sets out where services should consult ICO guidance for further information on data protection requirements. Further information on some of business F's data protection considerations is provided by the ICO below.

Data Protection

1.27. While the UK General Data Protection Regulation ('UK GDPR') does not require age assurance methods to be 'highly effective' in the same way as the OSA, all age assurance methods involve the processing of personal data and are subject to the requirements of data protection law.

1.28. As a service not intended for children, the Children's Code will not apply to business F if their age assurance method **effectively restricts** children from accessing their service. As Ofcom's guidance states, effectiveness, therefore, should be evaluated based on the **level of certainty** business F's method provides in confirming a user is 18+. Their assessment of effectiveness should also consider that the bill payer and the user of the phone are different.

Assessing Risk

1.29. Under Article 35 of the UK GDPR, a Data Protection Impact Assessment ('DPIA') is required when processing activities are **likely to result in a high risk** to the rights and freedoms of individuals. Given that business F's platform involves age verification to prevent children from accessing the service, it may be considered high-risk processing, particularly due to the potential risks to children's privacy and safety. As such, the ICO recommends that business F complete a DPIA.

1.30. Within business F's DPIA, they should **justify** their rationale for selecting their age assurance approach, include evidence on the level of certainty it provides using quantitative and qualitative data (e.g., lab test performance and indications of real world/live performance), and identify and address any risks associated with their chosen method, such as the potential for users to circumvent access and the

potential harms to them. Business F should also explain why their age assurance approach is proportionate to the risks.

1.31. Additionally, business F should consider the risk of excluding certain users if they rely solely on mobile phone verification. While it is crucial to avoid introducing an age assurance method that might allow children to access their service, it is also important to recognise that sole reliance on mobile phone verification could prevent access to 18+ users who do not hold mobile contracts.

Further Data Protection Considerations

1.32. The DPIA is also a tool for business F to explain how their approach meets wider data protection requirements. In particular under data protection law, services must ensure that the amount of personal information collected to verify or assure a user's age is proportionate. As such, the DPIA should include details about business F and business F's identity service providers' controllership role in the age assurance process. It should also include how long the information will be retained, how business F will inform users about this processing, business F's lawful basis for processing, and how users can exercise their individual rights. In particular, business F must provide tools so that users can challenge age assurance decisions and make these tools accessible and prominent.

1.33. Transparency is crucial in ensuring that users fully understand how their personal data will be handled. Clear and transparent privacy policies are essential for addressing data sharing with third-party identity providers and ensuring compliance with UK GDPR. These policies must provide detailed information on how user data will be collected, processed, and shared with any third parties involved in the age assurance process, such as identity providers. Users should be made aware of the types of personal information being shared, the specific purposes for which it is being used, and how it will be protected. The policies should outline retention periods, ensuring that data is only kept for as long as necessary to fulfil the purpose of age verification.

1.34. When sharing user data with third-party identity providers as part of an age assurance process, it is important to establish clear data sharing agreements to ensure that all parties involved comply with UK GDPR and other relevant data protection regulations. These agreements are essential for managing the relationship between business F's platform and the third-party providers, ensuring

that the processing of personal data is lawful, transparent, and secure.

Further Information

Online safety

1.35. Ofcom recommends using its dedicated Online Safety Regulation Checker tool, which can help business F determine whether a service falls under the classification of a 'pornography service' in addition to being a U2U service.

1.36. Ofcom also recommends the Guide for services: complying with the Online Safety Act - Ofcom and toolkit which provides a step-by-step interactive guidance on what business F needs to do to comply with the OSA.

1.37. Additionally, Ofcom has published a quick guide on implementing highly effective age assurance that provides an overview of the new rules and outlines steps that companies need to take to ensure they are complying.

1.38. Ofcom has published two statements which set out the obligations for providers of U2U services like business F have in respect of:

- **Illegal harms** statement - Providers of U2U services now have a duty to assess the risk of illegal harms on their services, with a deadline of 16 March 2025. Subject to the Codes completing the Parliamentary process, from 17 March 2025, providers will need to take the safety measures set out in the Codes or use other effective measures to protect users from illegal content and activity.

- **Age assurance and children's access** statement – Providers of U2U services in scope of Part 3 of the OSA must carry out a children's access assessment by 16 April 2025 to determine if they are likely to be accessed by children.

1.39. All services that allow pornography (Part 3 U2U services)[6] must implement highly effective age assurance to ensure that children are not normally able to access pornographic content by July 2025 at the latest.

Data protection

1.40. The ICO recommends business F review the ICO's Children's Code and ICO's guidance on Age Assurance for the Children's Code. The ICO has also published FAQs and case studies on services which are 'Likely to be accessed' by Children –

[6] For services which publish or display pornography (Part 5 services), the duty to implement highly effective age assurance came into effect on 17 January 2025, so providers should act immediately.

FAQs and Case Studies.

Joint guidance

1.41. Ofcom and the ICO work together through the DRCF to ensure regulatory alignment of age assurance. Under the Digital Regulation Co-operation Forum (DRCF), Ofcom and the ICO jointly commissioned research to explore the attitudes of children and parents/carers to age assurance methods and where they see the balance of trade-offs between considerations such as privacy, online safety and ease of use.