The Information Commissioner's response to Ofcom's consultation on guidance for service providers publishing pornographic content

About the Information Commissioner

The Information Commissioner's Office (the ICO) has responsibility for promoting and enforcing data protection and information rights. This includes responsibilities under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), the Freedom of Information Act 2000 (FOIA), the Network and Information Systems Regulations 2018 (NIS), the Environmental Information Regulations 2004 (EIR) and the Privacy and Electronic Communications Regulations 2003 (PECR).

The ICO is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. It also provides guidance and support to individuals and organisations and takes appropriate action where the law is broken. The ICO's strategic objectives include safeguarding and empowering people and empowering responsible innovation. Protecting children's privacy is a priority area for the ICO.

The Data Protection and Digital Information Bill was reintroduced in the Houses of Parliament on 8 March 2023. When the Bill becomes law, it will amend elements of the DPA 2018 and the UK GDPR relevant to this response. This response was written in line with the current applicable law at the time of writing.

Data protection and online safety

As the bodies responsible for regulating data protection and online safety in the UK, the ICO and Ofcom demonstrated their shared commitment to protecting people online by publishing a joint statement in November 2022.

The statement recognised that online safety and data protection interact in a variety of ways, including where age assurance is used. It set out our overall ambition to ensure coherence across online safety and data protection requirements and promote compliance with both regimes. We said that we want providers of online services of all sizes to comply with their obligations and to continue to innovate and grow, supported by regulatory clarity and free from undue burden.

Developing an aligned approach to the regulation of age assurance is a priority for both organisations. The ICO recognises the importance of consistent messages to businesses, and we are keen to continue working hand in hand with Ofcom to ensure that all children enjoy a safe online experience.

As part of that commitment Ofcom has engaged with us from the early stages of its development of this guidance and we also involved Ofcom in the development of our updated Commissioner's Opinion on age assurance for the Children's code (the Opinion).

We are pleased that the guidance reminds service providers that they should familiarise themselves with data protection legislation and how to apply it to age assurance methods by consulting our guidance. Section 6 of the Opinion sets out our expectations for age assurance and data protection compliance, including how the data protection principles apply.

The ICO's role in relation to age assurance and the Children's code

The ICO regulates age assurance in the following ways:

- Age assurance solutions must be designed and deployed in compliance with data protection law and follow a data protection by design approach. This includes where age assurance is required by the Online Safety Act 2023 (OSA).

- Where age assurance is used to support conformance with the ICO's Children's code (which is underpinned by data protection law) it should enable services to establish age with a level of certainty that is appropriate to the risks that arise from data processing.

The ICO's Children's code is a statutory code of practice for information society services[1] that are likely to be accessed by children. The code contains fifteen standards that information society services should conform to, to comply with their data protection obligations to protect children's data online. Standard 3 requires services that are likely to be accessed by children to either establish the age of users with a level of certainty appropriate to the risks arising from their data processing or alternatively to apply the standards of the code to all users.

The ICO published an initial opinion setting out the Commissioner's expectations for age assurance under the Children's code in October 2021 and updated the opinion in January 2024[2]. The Opinion explains how age

[1] An information society service is "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services."
[2] Where this response refers to the Opinion, it is referring to the updated version.

assurance can form part of an appropriate and proportionate approach to reducing or eliminating the personal information risks that children face online. It also sets out the ICO's expectations for data protection compliance when age assurance is deployed (including where it is required under the OSA).

We support the OSA requirement for services to use age assurance to ensure that children are not normally able to encounter regulated provider pornographic content. The processing of children's data by adult sites is a valid and significant concern and we recognise that preventing child access to such sites will also help to protect children from data protection harms. In our guidance about the "likely to be accessed" standard under the Children's code we say that if it would not be appropriate for children to access a service (e.g. because the service is targeted at adults), the focus should be on preventing child access. Part 5 of the OSA aligns with our guidance.

Age assurance deployment considerations: consultation questions 3-7

Question 3: Do you have any comments on our proposed guidance in respect of the kinds of age assurance which could be highly effective? If you consider there are other kinds of age assurance which have not been listed that you consider could fulfil the proposed criteria, please identify these with any supporting information or evidence.

We are pleased that the guidance recognises that all age assurance methods involve the processing of personal data and are subject to the requirements of the data protection regime. In particular under data protection law, services must ensure that the amount of personal information they collect about a person to verify or assure their age is proportionate. Where less intrusive – but still highly effective – methods are available, they should be used.

In section three of the Opinion we set out four main approaches to age assurance for the purpose of conformance with the Children's code (age verification, age estimation, self-declaration and waterfall techniques and age buffers).

The Opinion explains the scope of age assurance measures that are currently available. Although it does not address the question of whether particular solutions are "highly effective" for the purposes of online safety compliance, Ofcom may find it a relevant resource when it finalises its guidance.

Question 4: Do you agree that service providers should use the proposed criteria (technical accuracy, robustness, reliability and fairness) to determine whether the age assurance they implement which is highly effective at correctly determining whether or not a user is a child? Please provide any information or evidence in support of your views.

Technical accuracy, robustness, reliability

The proposed criteria align with the approach that we have set out in the Opinion. We say that information society services should ensure that any age assurance system they implement has an appropriate level of technical accuracy, reliability and robustness for the purposes of conforming to the Children's code. We also state that information society services must be aware of the specific risks that could arise from the deployment of age assurance such as:

- levels of inaccuracy which may be unsuitable given the purpose;
- unfair exclusion of marginalised groups due to inaccuracy of the solution or reliance on official documentation; and
- likely/ known circumvention of the approach.

The part 5 guidance and data protection law will therefore expect services to explain their chosen age assurance approach by applying similar criteria (although data projection law does not require age assurance methods to be "highly effective" in the same way as the OSA). We consider that this similarity in approach will help to secure regulatory alignment.

The proposed criteria in the draft guidance are not limited to assessing the chosen age assurance method in isolation, but also cover how it is used. We agree that any assessment made by a provider should be informed by multiple, inter-related criteria rather than being based solely on meeting a threshold for a single accuracy measure. In 2023 ICO and Ofcom jointly commissioned a piece of research into the measurement of age assurance technologies which reached similar conclusions.

We agree with the position in the guidance that any assessment of effectiveness should relate to the performance of the age assurance process as a whole and recognise this may involve 'trade-offs' between how well individual methods perform against each of the proposed criteria. We encourage providers of age assurance solutions to provide details of their solution's performance against the measures (i.e. lab test performance and indications of 'real world/live' performance).

Fairness

The draft guidance says that fairness describes the extent to which an age assurance method avoids or minimises unintended bias and discriminatory outcomes.

Data protection law also has a fairness requirement which includes that risk of bias and discrimination must be minimised. However, fairness under data protection law is broader. It means that a service must only process personal data in ways people would reasonably expect and which does not have an unjustified adverse impact on them. In order to make such an assessment, services need to consider whether such processing is necessary and proportionate.

In our view the fairness criterion outlined in the part 5 guidance should align with the requirements of fairness under data protection law so that services are clear that the requirements across the regimes are consistent.

Question 5: Do you have any information or evidence on the extent of circumvention risk affecting different age assurance methods and/or on any steps that providers might take to manage different circumvention risks for different methods?

We do not have further evidence on the extent of circumvention risk; however it is clear that the form such risks will take will vary considerably based on the methods described in the guidance.

For any technical risk of this kind, it is important for companies to comply with the data protection principles, specifically:

- the security principle, and
- the accountability principle.

The Opinion explains how companies can comply with these principles when deploying age assurance systems. When assessing security risks, companies should also refer to our guidance on AI and data protection and Biometric recognition guidance as appropriate.

Providers of age assurance systems will have varying ways to address their exposure to circumvention risk depending on whether their solution;

a) provides an end-to-end service with a direct relationship with the person proving their age (i.e. computer-vision based approaches like facial age estimation or photo-ID matching); or
b) is a discrete service relying on a wider supply chain or specific external providers (MNO, credit card checks, open banking or digital identity).

In the first scenario, there are existing guidelines around forms of biometric presentation attack (IS BS ISO/IEC 30107-3:2017) albeit the ability to test for all of these forms of attack is yet to be standardised.

There are also existing processes and information sources to interrogate the trustworthiness of specific official documents, such as GPG 45, as well as commercial products for trends in fraudulent identity documents.

These changes may be relatively simple for a provider to implement.

However, where solutions rely on the verification and authentication approach taken by another party (i.e. credit card checks or MNO) then age assurance providers are reliant on the outcome of a check undertaken by someone else. Any assessment of the robustness of a specific solution presupposes a level of transparency with all partners, where such a solution relies on a verification check made by someone else.

This presents a different challenge for providers, who will need regular diligence checks to consider the specific circumvention risks for their product, and reasonable, available methods to address them.

We acknowledge that Ofcom's concern is to mitigate circumvention attempts that are easily accessible to children, and where it is reasonable to assume that children might use them. What is 'reasonably available' to children will be a dynamic concept, particularly with the pace of technological change.

Question 6: Do you agree with our proposed guidance that providers should consider accessibility and interoperability when implementing age assurance? Please provide any information or evidence in support of your views.

We support Ofcom's promotion of accessibility. Accessibility means that age assurance should be easy to use and should work effectively for all.

Accessible AI-based age assurance approaches will support compliance with the first data protection principle (which requires processing to be lawful, fair and transparent), specifically considerations around data protection fairness.

Our guidance on Biometric recognition and AI and data protection both provide further detail on how organisations should approach fairness when deploying AI-based solutions.

The proposal that services should offer users a choice of several effective age assurance solutions could have a privacy-enhancing impact. Reliance on a single method increases the risk of circumvention, and the associated lack of protection for children's data online. This is supported by our joint research with OFCOM into families' attitudes to age assurance.

We agree that interoperability will be an increasingly important feature of age assurance approaches as the market continues to develop.

Question 7: Do you have comments on the illustrative case study we have set out in the guidance? Do you have any supporting information or evidence relating to additional examples of how

the criteria and principles might apply to different age assurance processes?

We are pleased that reference is made to the transparency requirements of data protection law in the case study, at point (2)(b).

The case study explains that the service provides two methods of age assurance for users to access, an age estimation or age verification method. Providing a range of measures can help organisations comply with data protection law by ensuring processes are fair while also minimising the personal information required to complete checks. For instance, the case study notes that people who are close in appearance to the age of 18 may be excluded from a service by an age estimation technique, so an age verification process can provide an alternative point of entry, making the process fairer.

The case study also makes reference to mitigations which can be considered for users who may be excluded by the use of either method. Such an approach aligns with the fairness principle under data protection law.

One omission from the case study, which Ofcom should consider including, relates to the data protection principle of accuracy. In the Opinion we explain:

> 'People have the right to challenge inaccuracies in their information which means you must consider any challenges to the accuracy.'

At section 4 of the case study, as a further mitigation, Ofcom should include a step which explains that services should provide a means for people to challenge age estimation or age verification results which they know to be inaccurate.

The Opinion contains advice where multiple forms of age assurance are being used which we refer to as the "waterfall approach".

Data protection and the part 5 record keeping duty: consultation questions 8-9

Question 8: Do you agree with our proposed guidance on the record-keeping duties? Please provide any information or evidence in support of your views.

Question 9: Do you have any comments on our proposed approach to assessing compliance with the duties on service providers who publish or display pornographic content, including on the

proposed examples of non-compliance? Please provide any information or evidence in support of your views.

The guidance sets out Ofcom's expectations for compliance with the record keeping duty under s81(4) OSA which includes the obligation to make and keep a written record of how services have had regard to privacy and data protection when deciding on the kinds of age assurance and how they are used.

UK GDPR sets requirements for organisations to keep records in relation to data protection in a number of ways. For example under current data protection law organisations must:

- perform a data protection impact assessment if their data processing is likely to result in a high risk to the rights and freedoms of individuals;
- keep a record of their data processing activities; and
- be able to demonstrate their compliance with the principles set out in Article 5(1) UK GDPR.

The ICO is keen to ensure that services understand how Ofcom's and the ICO's regulatory remits interact. We think that the guidance makes the division of regulatory responsibilities clear. However should consultation responses indicate that this is not the case, we are committed to engaging with Ofcom to ensure that the final guidance is clearer.

As paragraph 5.24 of the draft guidance makes clear, Ofcom will consider whether service providers have kept a written record of how they have had regard to privacy and data protection requirements in making decisions around age assurance. The ICO is the regulator that determines compliance with data protection law (and PECR, where relevant). These remits dovetail with each other but they are distinct.

The ICO will not opine on whether a written record is sufficient to meet the OSA duty and we would not expect Ofcom to opine on questions of data protection compliance. We are pleased to note that the guidance provides that where Ofcom has concerns that a provider, based on its written record, has not complied with its obligations under data protection law, it may refer the matter to the ICO.

We are also pleased to see that the guidance recommends that consulting ICO guidance and following data protection accountability requirements can help services to meet their online safety record keeping duty. These suggestions will help to ensure coherence across the regimes. However, as stated above, the final determination of data protection regulatory compliance is for the ICO.