Information Commissioner's opinion:

Age Assurance for the Children's Code

14 October 2021

Information Commissioner's Office

Contents

1. Executive summary

1.1 The Commissioner's work to protect children's data online

The Children's code (formally known as the Age appropriate design code) is a statutory data protection code of practice. It applies to providers or Information Society Services (ISS)[1] likely to be accessed by children, such as apps, online games, and web and social media sites.

The code contains 15 standards of age appropriate design. The code aims not to protect children from the digital world but to protect them within it by ensuring online services are designed with children in mind. The code entered into full effect from 2 September 2021.

One of the standards is age appropriate application, and taking a risk based approach to recognising the individual age of users and apply the Code's standards to children. The Commissioner recognises that age assurance may require processing of personal data beyond that involved in the delivery of a core service. However, the risks to children online are very real. This Opinion explains how age assurance can form part of an appropriate and proportionate approach to reducing or eliminating these risks and conforming to the code.

As part of the Digital Regulation Cooperation Forum (DRCF) the ICO and Ofcom are working together to understand and address the broad range of online safety risks for children online and to ensure coherence between different regulatory regimes.

1.2 What is the purpose of this Opinion?

This Opinion is for providers of ISS in scope of the code, and providers of age assurance products, services and applications that those ISS may use to conform with the code. It sets out how the Commissioner currently expects ISS to meet the code's age-appropriate application standard. It outlines a risk-based approach for organisations to apply age assurance measures that are appropriate for their use of children's data and organisational context.

The code sets out guidance on how to comply with the UK GDPR. Organisations must also consider the ICO's general guidance.

For ease of reference we use:

- a child (as defined in the code) as any individual under the age of 18 years;

[1] 'Information Society Service' is defined as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services." See Services covered by this code | ICO

- "organisations" to refer to providers of ISS and age assurance services collectively, as the nature of the relationship between them (controller-processor or joint controllers) may vary depending on circumstances[2]; and
- ISS activities to refer to processing of personal data for the purpose of providing the ISS.

1.3 What is age assurance?

"Age assurance" refers collectively to approaches used to:

- provide assurance that children are unable to access adult, harmful or otherwise inappropriate content when using ISS; and
- estimate or establish the age of a user so that ISS can be tailored to their needs and protections appropriate to their age.

We use two additional terms throughout this Opinion that describe different age assurance approaches:

- **Age verification:** Determining a person's age with a high level of certainty by checking against trusted, verifiable records of data.
- **Age estimation:** Estimating a person's age, often by algorithmic means. Outputs vary from a binary determination as to whether someone is or is not an adult, through to placing an individual in an age category.

Age verification is commonly used to establish whether someone is an adult, particularly where a high degree of certainty is required. For example, to ensure children are not able to access age-restricted products and services.

Some products and services have age guidance or restrictions lower than 18. It is beyond the scope of this Opinion to cover this in detail, but age assurance can still be applied.

A range of approaches to age estimation are in use and evolving. These are used for a variety of applications, including for risk assurance and management of ISS and to support personalised advertising and service personalisation.

1.4 What is an Opinion and why are we publishing this now?

Article 58(3)(b) of the UK General Data Protection Regulation (UK GDPR) and section 115(3)(b) of the Data Protection Act 2018 (DPA 2018) allow the Information Commissioner to issue Opinions to Parliament, government, other institutions or bodies as well as the public, on any issue related to the protection of personal data.

The Commissioner can issue Opinions on her own initiative or on request.

[2] Controllers, joint controllers and processors | ICO

Stakeholders engaged during the code's transition period have sought further information to inform their approach to age assurance, which remains challenging for many organisations. In particular, organisations have sought more clarity from the Commissioner on:

- the levels of risk arising from different types of data processing and the commensurate level of age certainty required to identify child users and mitigate the risks;
- the level of certainty that various age assurance solutions provide, and confirmation of which providers or types of solutions comply with data protection requirements; and
- how to collect the additional personal data required for age assurance while complying with the data minimisation principle.

This Opinion provides the Commissioner's current view on these issues, including how organisations can ensure age assurance is done in a compliant way. It is based on existing legislation, standards, guidance and developments as at the time of publication. It may inform the Commissioner's approach to regulatory action relating to the code.

We will review this Opinion as part of the planned, overall review of the Children's code in September 2022. In the meantime, we will continue to engage with stakeholders to gather evidence and feedback to inform this review. The Commissioner reserves the right to make changes or form a different view based on further findings or changes in circumstances. For example, the Commissioner acknowledges that the age assurance market is developing rapidly and will keep these issues under review as a result.

1.5 What are the Commissioner's expectations for age-appropriate application in the Children's code?

Standard 3 of the code on age-appropriate application requires organisations to:

> "Take a risk based approach to recognising the age of individual users and … effectively apply the standards in this code to child users. Either establish age with a level of certainty that is appropriate to the risks to the rights and freedoms of children that arise from your data processing, or apply the standards in this code to all your users instead."[3]

The Commissioner's expectations for conforming with this standard are set out in the table below. As noted in standard 2 of the code,[4] ISS likely to be accessed by children must carry out a DPIA which includes an assessment of the risks to children that arise from their data processing.

[3] 3. Age appropriate application | ICO
[4] 2. Data protection impact assessments | ICO

Children's risk level	Risk criteria	Age assurance expectations
High	ISS activities which are likely to result in high risk to children's rights and freedoms.	If any high risks cannot be mitigated, then they should consult with the ICO prior to commencing the ISS activities, in line with Article 36 of the UK GDPR[5]. Organisations should either: a) apply all relevant code standards to all users to ensure risks to children are mitigated; or b) introduce age assurance measures that give the highest possible level of certainty on age of users. This may take into account the products currently available in the market, and the potential risk to children.
Medium or low	ISS activities which are likely to result in medium or low risks to children's rights and freedoms.	Organisations should either: a) apply all relevant code standards to all users to ensure risks to children are low; or b) introduce age assurance measures that give a level of certainty on the age of child users that is proportionate to the potential risks to children.

Age assurance should be used to minimise risks to children. It should also ensure relevant aspects of the ISS (eg privacy information) which children are intended to access, are appropriate to those users.

Annex 1 summarises the steps that organisations should follow to decide whether age assurance is applicable to their ISS. Annex 2 provides further details about current and emerging approaches to age assurance.

[5] Do we need to consult the ICO? | ICO

1.6 What data protection principles must age assurance providers meet?

Processing of personal data for the purposes of age assurance must comply with the UK GDPR and DPA 2018, and respect the privacy of children during both the development and application of any technique.

Organisations must also assess the risks and potential harms arising from age assurance. They must put in place appropriate technical and organisational measures to safeguard children and adults from these risks. Organisations must ensure that their use of age assurance complies with the following principles:[6]

- **Lawfulness** – there must be an appropriate lawful basis for the processing.
- **Fairness** – including the ability for users to challenge incorrect decisions;
- **Transparency** – children and adults must be aware that age assurance is being done, and how decisions are made.
- **Purpose limitation** – do not use data obtained for age assurance for any other purpose.
- **Data minimisation** – use only the data that is necessary for the age assurance and do not retain it longer than needed.
- **Accuracy** – data must be accurate and data subjects must be able to correct inaccurate data and challenge incorrect decisions.
- **Storage limitation** – data for age assurance should not be kept for any longer than necessary.
- **Integrity and confidentiality (security)** – organisations must ensure that any data processing in the context of age assurance is done securely using appropriate technical and organisational measures.

1.7 Next steps

The Commissioner recognises the balance required to protect privacy whilst protecting children in a better online world. This Opinion sets expectations to support the development of age assurance methods in a way that ensures data protection by design and default.[7]

The code entered into full effect from 2 September 2021, including standard 3 on age appropriate application. While the Commissioner appreciates the developments in age assurance techniques, technology and policy, more needs to be done to ensure these respect and comply with data protection law. The

[6] The principles | ICO

[7] 'Data protection by design and default' is a requirement in the UK GDPR whereby organisations must integrate data protection concerns into every aspect of their processing activities. It is a key element of the UK GDPR's risk-based approach and its focus on accountability. Further information can be found at Data protection by design and default | ICO

Commissioner supports this work but expects to see continued steps being taken in the maturity of organisations' conforming with the code.

Organisations should evidence and record their assessment of risks and decisions they take, including on the age appropriate application standard. This will ensure accountability for the decisions taken and enable organisations to demonstrate their approach, even if it is evolving. This is also evidence the ICO can consider if a complaint is brought about an ISS or it comes to the ICO's attention.

A summary of the expected economic costs and benefits of age assurance is included at Annex 3.

Due to the rapidly evolving state of the age assurance market, wider legislative proposals and developing policy landscape, we will revisit this Opinion in line with the planned review of the Children's code in 2022. We will continue to engage with key stakeholders, including Ofcom, the Children's Commissioner, Government, industry and civil society to develop our understanding of emerging age assurance approaches. It is likely that our work with Ofcom will become more extensive given their role as regulator for video sharing platforms (VSPs)[8] and future regulator for online safety. We will work together with Ofcom and other regulators to ensure a coherent approach, particularly in the event that we engage with the same ISS at the same time.

As part of this, we welcome engagement from interested parties, particularly about evidence of emerging age assurance techniques and their accuracy. This will help businesses to ensure that age assurance does not degrade the experience of using their ISS at the same time as facilitating the optimal solutions and protections for children.[9]

The Commissioner is also keen to support the development of age estimation approaches and data protection by design. This will build on the work we have done in our regulatory Sandbox and our approval of certification schemes that address age estimation, UK GDPR compliance and conforming with the code.

The Commissioner will take action in the event that personal data is misused under the guise of or during processing for age assurance.

[8] Ofcom regulates VSPs established in the UK to ensure they take appropriate measures to protect children from potentially harmful material in videos. More information about Ofcom's VSP regulation can be found here

[9] Blog: How the digital design community can help shape the ICO's work on the Children's code | ICOS

2. Introduction

An overarching aim of the code is to ensure that all children are given an age-appropriate level of protection.

Age assurance is an important part of the most fundamental standard in the code: considering the best interests of the child.[10] The United Nations Convention on the Rights of the Child (UNCRC) (and the code) states that:

> "In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration."

While the code does not mandate the adoption of any one solution, age assurance techniques can play an important role in how you achieve this outcome. For example, age assurance may:

- protect children from harms arising from the processing of their personal data;
- enable information to be provided to children about how their data will be collected, processed and used, in a way appropriate to their age group whilst using ISS; and
- protect children from intrusive activities such as profiling, marketing and behavioural advertising.

However age assurance must be used carefully as it carries its own types of risk. For example, it:

- may be disproportionately intrusive. For example, age verification checks often require access to official data or documentation which can include special category data;
- may introduce risks of bias and inaccuracy. For example, some emerging approaches to age estimation are based on profiling or facial analysis using AI;
- may result in exclusion or discrimination of already marginalised groups due to bias, inaccuracy or requirements for official documentation. Those in more deprived socio-economic groups are more likely to lack requisite documentation, and more likely to be affected by algorithmic bias. Non-white ethnicities and people with disabilities are over-represented in these groups. Individuals may be unable to use some types of age assurance due to physical or cognitive reasons and risk being excluded from services they are entitled to access;

[10] 1. Best interests of the child | ICO

- is not fool-proof. Any approach has some risk of incorrectly classifying a child as an adult or as an older child. This could potentially allow them access to inappropriate or harmful services or material. Conversely, an adult may be incorrectly classified as a child, and be denied access to services they are legally entitled to use; and
- some methods can be circumvented. For example, a child or parent could provide false information in a self-declaration or a child could log into their parent's account to complete account confirmation.

The onus is on organisations to show that their approach is lawful, effective and proportionate. This Opinion sets out how organisations should approach age assurance and compliance with the code.

2.1 Scope of this Opinion

This Opinion is aimed at ISS and age assurance providers. It builds on the guidance in standard 3 of the code. It describes a risks and standards based approach to age assurance that will help ISS choose the right approach for their circumstances in order to meet that standard.

This Opinion applies specifically to the use of age assurance to support ISS' to conform with the code. It does not apply to the use of age assurance in circumstances outside the code, such as in physical spaces like retail settings or as a means of restricting access to ISS that provide adult content or services. We are working in co-operation with other regulators to ensure a coherent approach.

This Opinion will be useful to those organisations who seek to use age assurance to prevent their services being accessed by children. For example, online retailers of alcohol. This will help them to comply with their obligations under the UK GDPR and wider regulatory frameworks. However, it is not written solely for these circumstances, so organisations will need to assess the relevance and applicability of this Opinion to their circumstances.

2.2 References to legislation

This Opinion relates specifically to:

- Data Protection Act 2018 (DPA 2018);
- UK General Data Protection Regulation (UK GDPR); and
- Privacy and Electronic Communications Regulations 2003 (PECR).

2.3 Methods of age assurance

Organisations have a fundamental choice when managing the risks posed to children by their ISS. They may choose to:

- use age assurance to identify children to a level of certainty proportionate to the risks of their using the ISS, and to ensure that the standards of the code are applied to all child users. For example, by providing a differentiated ISS, or not allowing children to access the ISS; or
- apply the standards of the code to all users of the ISS if they are unable (or do not wish) to use age assurance.

There are four main approaches to age assurance as described below. Each approach has strengths and drawbacks, and can be used to manage different levels or types of risk. In some circumstances, a combination of different age assurance approaches may be effective. This depends on the nature of the risks being addressed and the potential harms to children linked to those risks. The Commissioner emphasises that the risks and harms faced by children online are real, and that age assurance can be an important part of an appropriate and proportionate response.

When deciding how to implement age assurance, organisations should consider whether less privacy-intrusive approaches can achieve the same objective.

2.3.1 Age verification

Age verification refers to determining a person's age with a high level of accuracy by checking against trusted records of data. Approaches to age verification include:

- **hard identifiers:** confirming age using solutions that link back to identity documents or officially held data, such as a passport or credit card. This can be done by the user, or another party, for example a parent, guardian or teacher; and
- **third party services:** age verification may be outsourced to a third party using any or all of the techniques listed.

Age verification offers a high level of certainty, but must be used in proportion to the identified risks to children. There is a risk of indirectly discriminating against individuals who lack the necessary documentation or data, such as credit history.

Organisations that do not intend to use age assurance must take alternative measures proportionate to the risk to children, such as applying the code to the whole of their ISS and all of their users. The flowchart at Annex 1 (below) illustrates this.

See Annex 2 (below) for further information on the use of age verification for age assurance in the code.

2.3.2 Age estimation

Age estimation refers to the estimation of a person's age, usually by algorithmic means. It is a catch-all term for a suite of AI-based or AI-assisted technologies that can estimate an individual's age within a margin of error. It may involve biometric data or profiling or both.

Age estimation:

- can provide more granular determination of age, allowing differentiation of service where this is helpful to users (eg enhancing the age appropriate user experience);
- does not require documentary evidence or checks of official databases and so may be designed in a more privacy-friendly way than age verification; and
- can be used to verify if users have been wrongly classified as children or adults, and their identity corrected, if employed in ongoing monitoring.

Age estimation techniques can accurately determine whether an individual's age is within a specified range. The range may be comparatively wide. For this reason, age estimation alone may not provide sufficient certainty for ISS activities which are high risk to children.

Age estimation based on profiling is likely to be privacy intrusive but can offer a means to automatically identify under-age users. Age estimation based on biometrics, such as facial or hand geometry, has the potential to be more privacy friendly if data minimisation and purpose limitation are applied rigorously.

The market for age estimation has the potential to develop rapidly, and the Commissioner will keep these issues under review. The Commissioner expects these technologies to be developed in line with the principles of data protection by design and by default. They should therefore come to fruition in a data protection-compliant way. The Commissioner will continue to engage with organisations to address age estimation, UK GDPR and code compliance. This builds on the work done in our Sandbox and approval of certification schemes.

See Annex 2 for further information on the use of age estimation for age assurance to conform with the code.

2.3.3 Account confirmation

Account confirmation enables an existing account holder to confirm that a user is over or under 18, or the age of the user. The ISS can then provide the user with an age-appropriate version.

For example, in a family account, the main account holder can confirm the age of the people using the other account profiles. The service can then be applied in an age appropriate way to each user.

Account confirmation is useful for lower risk services, or if done in addition to other age assurance methods. It has limitations that mean it is unlikely to be sufficient when used as the only age assurance measure in high risk ISS activities. This is because it:

- requires active engagement, willingness and a level of IT knowledge from the parent or guardian;
- relies on notifications to parents when action is required, which may lead to fatigue;
- depends on the parents having the capability and capacity to manage their child's ISS experience (and thus carries some risk of discrimination if relied upon solely);
- may require the parent's age or identity to be confirmed if they are used to manage access by children to higher risk services;
- can be bypassed by knowledgeable children or by parents willing to put in an inaccurate age to allow a child to use an inappropriate service, putting the ISS at risk of breaching the code; and
- may cause conflict between parents or guardians if there is disagreement between them.

Account confirmation may involve processing the data of both the original account holder (usually a parent) and the confirmed account holder (usually a child).[11]

See Annex 2 for further information on the use of parental controls for age assurance to conform with the Children's code.

2.3.4 Self-declaration

Self-declaration is where a user states their age but does not provide any evidence to confirm it.

It may be suitable for low risk ISS activities or when used in conjunction with other techniques. It does not significantly mitigate risk as it is based on trust and can be circumvented, even if additional technical measures are applied. However, it enables the ISS to be customised to the needs of different age groups where the risks to children are low. For example a website whose main purpose is just to provide useful information.

There are technical measures that can strengthen self-declaration. For example:

[11] 11. Parental controls | ICO

- preventing the user from immediately attempting to re-register if they are denied access on first declaration; or
- closing the accounts of users discovered to be underage.

These measures are not difficult to bypass for determined or knowledgeable children.

Self-declaration can be minimally intrusive. For example, users are asked to put themselves in an age bracket rather than provide date of birth. However, consideration needs to be given to the effectiveness of this, particularly about the age brackets chosen.

2.4 Age assurance and discrimination

Age assurance may produce discriminatory outcomes. Two examples are listed below:

- Age verification usually depends on the user having ready access to official documentation, or a credit history. This is an issue for:
    - young adults;
    - those with protected characteristics; and
    - those from deprived backgrounds (in which people with disabilities or of non-white ethnicity are over-represented), who may not have access to such documentation and so be unable to access the ISS.
- Age estimation carries risks from algorithmic bias. Systems based on biometrics such as hand or facial structure may perform poorly for people of non-white ethnicity, or for those with medical conditions or disabilities that affect physical appearance. There is also a risk from newer techniques that have not been effectively tested or screened for these risks.

The risk of discrimination is heightened for those individuals with multiple protected characteristics, so organisations must consider how to mitigate those risks.

Discriminatory outcomes may be in breach of both the Equality Act 2010, and UK GDPR (since processing with discriminatory outcomes is unlikely to be fair).

Organisations must consider their obligations under the Equality Act. As part of this, it is very important that age assurance incorporates reasonable adjustments for disabled persons, such as offering alternative methods for age assurance. Also, there must be an accessible process for users to challenge an incorrect age assurance decision.

3. How we expect age-appropriate application to be carried out

This chapter outlines our expectations of how an ISS provider should approach age assurance when applying the code.

Standard 3 on age-appropriate application advises organisations to:

> "Take a risk based approach to recognising the age of individual users and … effectively apply the standards in this code to child users. Either establish age with a level of certainty that is appropriate to the risks to the rights and freedoms of children that arise from your data processing, or apply the standards in this code to all your users instead."

In the following sections, we outline our expectations for organisations to take a risk-based approach to age assurance when applying the code to its ISS.

3.1 How the code defines risk

Many data-related risks faced by children are similar to those faced by adults. However, in many cases both the likelihood and severity of harms are greater for children than adults.

Recital 38 of the UK GDPR emphasises that:

> "children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing…"

These protections and safeguards are collectively articulated by the code's standards.

Standard 1 states that:

> "The best interests of the child should be a primary consideration when you design and develop online services likely to be accessed by a child."

In order to apply this standard, the organisation must use the UNCRC to identify and assess data-related risks to children. The UNRC describes children's universal rights and freedoms, which when contravened are likely to harm children.

The ICO has developed a "Best interests framework" to support organisations to apply the UNCRC and identify where ISS activities pose risks to children[12] For example:

- life, survival and development (Article 6 of the UNCRC): geolocation data sharing leading to physical harm (for example through stalking);
- protection from economic exploitation (Article 32 of the UNCRC): personalised advertising or sharing of children's data for commercial gain without safeguards; and
- development and preservation of identity (Article 8 of the UNCRC): sharing identity data with third parties or profiling that infers identity characteristics without safeguards.

The code and the Best interests framework, only cover risks that arise from processing personal data. Risks to children not related to data processing are outside the scope of the code. For example, general online safety risks that data plays no role in.

3.2 ISS activities likely to result in high-risk to children

The code sets standards for certain ISS activities which are likely to result in high-risk to children.[13]

The nature of some ISS activities means they carry more inherent risk than others. For example, where they are more intrusive, opaque, or inform decisions that have significant impacts on individuals.

The Commissioner publishes guidance on data processing activities that are considered "likely to result in high risks" to data subjects (covering both adults and children).[14] This includes large-scale profiling, invisible processing and tracking.

The code draws upon this list and evidence gathered through the code consultation process and the ICO's Towards a better digital future[15] research. It sets standards for certain data processing where risks to children are likely to be high, for example around profiling and data sharing.

Taking all these areas into account, the Commissioner considers that the following ISS activities are likely to result in high risks to children:

- **Large-scale profiling of children.** For example, to identify children as belonging to particular groups, for automated decision-making, analysing social networks, or to infer interests and behaviours.

[12] https://ico.org.uk/media/for-organisations/documents/2618906/childrens-code-harm-framework-beta.xlsx
[13] 2. Data protection impact assessments | ICO
[14] Examples of processing 'likely to result in high risk' and so require a Data Protection Impact Assessment. ICO
[15] Towards a better digital future Informing the Age Appropriate Design Code (ico.org.uk)

- **Invisible processing of children's data** that the ISS did not obtain directly from users. Examples include list brokering, data sharing with third parties, and online tracking of children.
- **Targeting of children for marketing and advertising.** For example, personalising marketing content based on children's data.
- **Tracking of children.** This includes the child's use of ISS and digital proxies for offline activity, such as geolocation. For example, web and cross-device tracking, fitness or lifestyle monitoring using connected devices and ISS reward schemes.
- **ISS activities with risks of physical or developmental harm to children.** For example, if there was a personal data breach or through data sharing (with third parties or other ISS users). For example, data that reveals children's physical location or health, or which could expose children to unsafe or age-inappropriate products and services.
- **ISS activities with risks of detrimental use.**[16] For example, processing which is demonstrably against children's wellbeing, as defined by other regulatory provisions, government advice, or industry codes of practice**.**

In a DPIA[17] (or another assessment) organisations may decide that some ISS activities are likely to result in a high risk to children.

Alternatively, organisations may decide that in their particular circumstances, the activities are not high risk in themselves, or that measures to mitigate the risk can reduce it to medium or low. In this case, we would expect to be provided with the organisation's DPIA or other supporting evidence to show how the risk has been assessed or mitigated or both.

3.3 Age assurance certainty and risk levels

3.3.1 High risk processing of children's data

For the purpose of the code, we define high risk activities as data processing that:

- the Commissioner considers "likely to result in high risk to children" (as set out in section 3.2); or
- the ISS' risk assessment indicates risks to children's rights and freedoms are high.

That is, the likelihood of harm to children occurring is high, or the impact of the harm is not minimal; or there is a reasonable possibility of serious harm occurring.

[16] 5. Detrimental use of data | ICO
[17] Standard 2 sets out that organisations should always carry out a DPIA.

ISS must either:

- apply all relevant code standards to all users to ensure risks to children are low, or;
- introduce age assurance measures that give the highest possible level of certainty on age of users – accounting for products currently available in the market, their organisation's technical capabilities and resources.

If neither of these approaches are taken, the Commissioner expects that organisations will consult with the ICO prior to commencing the processing, as there are likely to be residual high risks to children. Failure to do so may be seen as an aggravating factor in any regulatory action the Commissioner takes. In addition, the ISS should have completed a DPIA. If they are unable to mitigate any high risks to children, they must have consulted the ICO prior to commencing the processing, in line with Article 36 of the UK GDPR[18]

Any data processing for age assurance must comply with UK GDPR. This includes all principles outlined in section 4 and be proportionate. Age assurance measures must not result in a net increase in risks to all data subjects (relative to the risks to children that would be present without the age assurance measure).

3.3.2 Other processing of children's data

Where an ISS assesses that the level of risk to children is below the thresholds set out above, it can:

- apply all relevant code standards to all users to ensure risks to children are low;
- introduce age assurance measures that give a level of certainty on the age of child users that is proportionate to the risks that arise from processing their data. This assurance should be used to minimise risks and ensure relevant aspects of the service (eg privacy information) are accessible and appropriate to those users; or
- self-declare, which may be appropriate for some low risk services (or enhanced self-declaration using technical measures – see Annex 2 for details). This is especially where there is minimal scope for services being tailored for different age groups.

The use of data processing for age assurance must:

- comply with UK GDPR, including all principles outlined in section 4; and
- be proportionate. Age assurance measures must not result in a net increase in risks to all data subjects (relative to the risks to children that would be present without the age assurance measure).

[18] Do we need to consult the ICO? | ICO

For the purposes of the expectations and definitions set out above, the Commissioner clarifies several key points.

ISS should conduct their risk assessment through their DPIA, and follow the relevant steps and standards outlined in the code's DPIA standard.[19] General information is also provided in the ICO's detailed guidance on DPIAs[20]

The expectations are for high-risk services to introduce measures with the "highest possible level of certainty on age of users" (as opposed to specifying specific appropriate measures). This acknowledges that the certainty of a given measure will vary across services. This is due to a range of factors including technical feasibility, whether a service is used by authenticated or non-authenticated users, and the age ranges and capabilities of users.

The Commissioner will take into account the products currently available in the age assurance marketplace when considering whether an organisation has conformed with the code. The Commissioner will also continue to take into account the impact of the potential economic burden our actions can place on organisations through her work, as outlined in the ICO's regulatory approach.[21]

The expectation of "highest possible" certainty on age of users for high-risk services reflects both of these commitments. The Commissioner will not expect services to implement age assurance measures that:

- are not currently technically feasible; or
- pose a significant and disproportionate economic impact on their business.

ISS will however be expected to demonstrate that they have considered all possible age assurance options. They should also evidence disproportionate costs, disproportionate impact on data subjects, or technical explanations for why they are not using age assurance measures that may provide higher certainty.

The ecosystem for age assurance standards is developing. The Commissioner will take into account adherence to such standards when considering whether ISS are deploying age assurance measures of an appropriate level of certainty.

3.4 Age-restricted services and the Children's code

For services that are age-restricted in law, the code should not lead to the perverse outcome of these providers having to make their services child-friendly, for example, adult content and services. Providers of such services should focus on preventing their access by children. We will continue to work with OFCOM and the DRCF to ensure that these broader online safety risks are managed. If a

[19] 2. Data protection impact assessments | ICO
[20] Data Protection Impact Assessments (DPIAs) | ICO
[21] ICO regulatory approach

service is not intended for children to use and is age-restricted, then the focus should be on preventing access. In this case, the code does not apply but services should make sure that their service is not likely to be accessed by children, either by ensuring it does not appeal to them, or that they cannot access it if it does.

4. Expectations for age assurance data protection compliance

This chapter outlines the main data protection principles and requirements that we expect to be taken into account in the context of age assurance. This covers only those relating to an organisations processing for age assurance (and not delivering the service or platform). The considerations set out are not specific to any particular approach or technology but apply wherever age assurance is used about the code. Those implementing age assurance systems therefore must:

- consider the risks to children that arise from their platform or service;
- determine whether age assurance of users is required; and
- select an approach that is appropriate and proportionate to the risk.

Age assurance providers should ensure that they embed data protection into the design of their products, services and applications.

4.1 Principles

Article 5 of the UK GDPR sets out seven key principles which lie at the heart of data protection. Organisations should follow these when processing any personal data. The Commissioner has published guidance on these principles[22]. This section of the Opinion provides key considerations about how these principles relate to age assurance. Note that UK GDPR considers lawfulness, fairness and transparency together as one principle. We have separated them here for clarity.

4.1.1 Lawfulness

Any processing of personal data must be lawful. This means organisations need to identify a lawful basis to process personal data for age assurance purposes.

Most lawful bases require processing to be necessary for a specific purpose. To be necessary, processing does not have to be absolutely essential, but it must be more than just useful and standard practice.

Age assurance must therefore be a targeted and proportionate way of achieving the objective of ensuring age-appropriate application of your services. The processing will not be lawful if you can reasonably achieve this purpose by other less intrusive means, or by processing less data.

Processing for age assurance that involves biometric data is discussed in section 4.2.1.

[22] The principles | ICO

The Commissioner has issued detailed guidance on the available lawful bases and an interactive tool[23] that can assist organisations to identify the most appropriate one for their circumstances.

If no lawful basis applies, then the processing is unlawful and infringes this principle.

4.1.2 Fairness

Any processing of personal data for age assurance must be fair. This means it must not be processed in a way that is detrimental or misleading and no user should be discriminated against. The Commissioner expects organisations using age assurance to take action to scrutinise and minimise any potential bias in their approach to age assurance. They should also continually seek to improve the performance of their approach in this area.[24]

In general, fairness means that organisations should only handle the personal data they are processing for age assurance, in ways that people would reasonably expect. They should also not use it in ways that have unjustified, adverse effects on them. ISS may wish to use market research or user testing to help establish reasonable expectations in this context. Standard 5 of the code requires that organisations should not process children's personal data in ways that are obviously, or have been shown to be, detrimental to their health or wellbeing. To do so would not be fair.

An important aspect of fairness is ensuring that users have an effective way to challenge an age assurance decision if they believe it is incorrect.

4.1.3 Transparency

Organisations need to be clear, open and honest about how they use personal data for age assurance purposes, and how they make decisions as a result. Standard 4 of the code provides advice on presenting this type of information to children.[25] ISS should consider how age assurance fits in to their overall user journey and experience to determine how and when it is best to provide users with this type of information.

Regardless of the method used for age assurance, it is important to explain clearly and appropriately to individuals:

- why an age assurance step is being used;
- what data is needed for age assurance;
- whether a third party will be used to carry out the age assurance check;

[23] Lawful basis interactive guidance tool | ICO
[24] Section 4.2 sets out additional considerations where age assurance uses AI.
[25] 4. Transparency | ICO and designing-data-transparency-for-children.pdf (ico.org.uk)

- how the data is used and how it will affect the user's experience of the platform or service;
- whether data collected for age assurance will be retained, how and why;
- how an incorrect age assurance decision can be challenged; and
- how they can exercise their data protection rights.

If an age assurance method involves automated decision-making, organisations must be able to explain how this decision is arrived at, in a way that users can understand.

Transparency is fundamentally linked to fairness. If organisations are not clear and transparent about how they will process users' personal data for age assurance, it is unlikely that their processing will be fair.

4.1.4 Purpose limitation

Personal data must only be processed for specific and legitimate purposes, and not further processed in a manner incompatible with those purposes. Purpose limitation is a fundamental aspect of transparency, fairness, and data protection by design.

Organisations implementing an age assurance system need to:

- be clear about what personal data it processes;
- be clear about why they want to process it;
- ensure they only collect the minimum amount of data they need to establish an appropriate level of certainty about the age of their users; and
- ensure they do not use personal data collected for these purposes for any other purpose, unless the new purpose is compatible.

Developers of age assurance systems need to ensure that they build their systems with data protection in mind.

Data collected for age assurance should not be re-used for purposes such as profiling for advertising, or in other ways that are incompatible with the purposes for which the data has been collected. The code provides guidance about purposes which are considered likely to be incompatible[26]. Standard 9 of the code notes that organisations should not share children's data unless they can demonstrate a compelling reason to do so, taking account of the best interests of the child.[27] Therefore, organisations need to ensure that they do not share children's age assurance data unless there is a compelling reason to do so.

[26] 12. Profiling | ICO
[27] 9. Data sharing | ICO

4.1.5 Data minimisation

Organisations using age assurance must apply data minimisation to their chosen approach. Any data processed for age assurance purposes must be:

- adequate – sufficient to properly achieve the stated purpose of age assurance;
- relevant – has a rational link to that purpose; and
- limited to what is necessary (ie is not processed more than is needed for that purpose).

UK GDPR requires organisations to:

- be clear about the purposes for which they collect personal data;
- only collect the minimum amount of personal data needed for those purposes; and
- only store that data for the minimum amount of time required.

Organisations need to differentiate between each individual element of their service and consider what personal data they need, and for how long, to deliver each one. Standard 8 of the code provides advice on meeting this requirement.[28]

The Commissioner recognises that age assurance may require processing of personal data beyond that involved in the delivery of a core service. However, the risks to children online are very real. The Commissioner considers that, provided this processing is limited to what is necessary and proportionate, the use of age assurance is, in many cases, likely to be an appropriate way of reducing the risk of harm to children online while complying with the data minimisation principle.

To ensure compliance with data minimisation requirements, organisations must ensure that they only use data necessary to undertake age assurance. What is necessary will be linked to what is proportionate for the circumstances. A service or platform that poses a low risk to children is likely to need to process less data to assess the age of users than one that poses a high risk to children. If reasonable adjustments for some users are required for equality purposes, organisations may need to collect more personal data than they would otherwise.

For example, in many cases organisations will not need to see a full passport or official document. This is because they can use a method of age assurance that processes less data whilst still proportionate to the risks faced by children. In a high risk scenario it may be necessary to collect more data to verify a user's age, compared to a low risk scenario. In either case, organisations need to

[28] 8. Data minimisation | ICO

justify why the data they want to process is necessary to achieve the purpose of age assurance.

The use of third-party suppliers has the potential to limit the data an organisation processes directly, and this may be a factor in its approach to data protection compliance. For example, an organisation may simply receive a 'yes or no' outcome of whether the user is under or over 18, rather than processing a copy of the user's passport or identity document. However, the organisation remains responsible for the processing activities overall, if the external supplier is processing personal data on the organisation's behalf to achieve this 'yes or no' outcome.

4.1.6 Accuracy

Accuracy is particularly important in the context of age assurance,[29] and organisations must monitor and consider carefully any challenges to the accuracy of data. Data subjects have the right to correct any inaccuracies in their personal data.[30] ISS developing in-house age assurance solutions should ensure they are tested for accuracy, and those using external solutions should seek evidence from their suppliers.

The two main incorrect outcomes for age assurance are:

1. an adult who is wrongly identified as a child, or a child wrongly identified as younger than they really are is denied access to a platform or service that they should be able to use legally, or gains access to child-only services or forums with a maximum age limit which may result in risks to the child users; or
2. a child who is wrongly identified as an adult or older than they are, is able to access a product or service that is restricted to adults or children of an older age.

A child who is able to access services intended for adults or older children may, for example, unwittingly consent to data processing that leads to inappropriate profiling. Organisations processing data for children under 13 where there is no evidence of informed parental consent are not processing the data legally. Conversely, adults may suffer detriment or harm if they are denied access to services they need.

With age estimation, there may also be a range of outcomes where older children are misidentified as younger, and vice-versa. There are some lesser, though still undesirable, consequences to this. For example, information about a platform or service and how it processes personal data could be provided in an age-inappropriate format if a child is identified as belonging to an incorrect age

[29] This section refers to accuracy in the context of data protection, however section 3.4 comments on the statistical accuracy of algorithms.
[30] Right to rectification | ICO

group. More seriously, it may lead to younger and more vulnerable children accessing parts of a platform or service that are not appropriate, putting them at risk of harm. More sophisticated approaches look for "red flags" that highlight potential errors in the original estimation.

However, no system is fool proof. Organisations implementing age assurance must consider the risk that age checks may be bypassed, and the harm that may result from doing so. They should also consider, for both age verification and age estimation approaches:

- how an adult or older child wrongly denied access to part or all of a platform or service can challenge a decision. For example, to comply with the right to rectification[31] and, in the case of automated decision-making, the UK GDPR Article 22 right to human review[32];
- how a child (or their parent or guardian) wrongly identified as an adult or older than they are, can challenge this outcome; and
- whether the potential harm to children accessing an inappropriate platform or service is sufficient to justify ongoing monitoring of users. For example, to identify children that may have wrongly gained access. Any such monitoring must comply with data protection requirements.

4.1.7 Storage limitation

Organisations must not keep any personal data for longer than it is needed. Organisations must be able to justify how long they keep data collected for age assurance purposes and they need a policy that sets out retention periods. The relative level of confidence in the accuracy of an age check does erode over time as age assurance technology and fraud prevention improve. To maintain accuracy, age assurance data should not be held longer than necessary.

Under UK GDPR, individuals including children have the right to erasure of data that is no longer required. Organisations must carefully consider any challenges to their retention of data collected for age assurance. Organisations should refer to ICO guidance on the right to erasure[33] and data retention[34] as these require consideration beyond the scope of this Opinion.

4.1.8 Security

Organisations must process personal data used for age assurance securely.[35] When implementing age assurance, organisations need to ensure that their system processes personal data securely. To ensure appropriate security, they should consider the specifics of the system and its intended outcomes, as well as

[31] Right to rectification | ICO
[32] The rights of individuals | ICO
[33] Right to erasure | ICO
[34] Principle (e): Storage limitation | ICO
[35] Security | ICO

the data involved. This should form part of their considerations about risk analysis, organisational policies, and physical and technical measures.

Organisations can consider the state of the art and costs of implementation when deciding what measures to take. However, the key is that any measures they put in place must be appropriate both to the circumstances and the risk the processing poses. If the potential risk to children is high, then organisations may have to put in place more costly security measures to protect them from those risks.

Both in-house and third-party solutions for age assurance should therefore demonstrate appropriate data security measures and accountability.

If using AI, organisations should consider the balance between transparency and security. For example, given sufficient technical information, there is a risk that a malicious actor could re-identify data subjects using a model inversion attack.[36]

The Commissioner has provided further information about AI and security in guidance on AI and data protection.[37]

4.1.9 Accountability

The accountability principle means that an organisation must be able to demonstrate how it complies with the law in its age assurance activities.

Organisations need to be able to demonstrate that their approach to age assurance is proportionate to the risks to children associated with a platform or service.

A DPIA is a key accountability tool. It is good practice to carry out a DPIA at an early stage in the design of any product or service that involves the processing of personal data (even if it is not a UK GDPR requirement). This applies for age assurance. Standard 2 of the code explains how DPIAs fit into the wider context of the Children's code.[38]

Another effective method of demonstrating accountability is the use of codes of conduct and certification mechanisms. These enable a flexible, risk-based and proportionate approach. For example, a standard[39] and certification scheme[40] has been in place for age assurance providers since 2018, with the latter being approved as a UK GDPR scheme in 2021. The Commissioner expects organisations that use age verification systems who are not certified to be able to provide other evidence that the checks they are using are effective.

[36] Privacy attacks on AI models | ICO
[37] Known security risks exacerbated by AI | ICO
[38] 2. Data protection impact assessments | ICO
[39] PAS 1296 - Age Check Certification Scheme (accscheme.com)
[40] Home - Age Check Certification Scheme (accscheme.com)

Age assurance may be unnecessary. For example, where an organisation demonstrates that the risks to children are low, and its platform or service in its entirety conforms to the code. Or, if all of the content or services provided by an ISS to all of its users conform to the code, it is likely that the disadvantages of age assurance would outweigh any benefit.

In addition to the above, there are a number of accountability measures that organisations must take (where applicable), including:

- adopting and implementing data protection policies;
- taking a data protection by design and default approach;
- putting written contracts in place with third party verification services that process personal data on their behalf (these may be processors or joint controllers depending on the exact circumstances of their relationship[41]);
- maintaining documentation of their processing activities;
- implementing appropriate security measures; and
- recording and, where necessary, reporting personal data breaches.

The Commissioner has published guidance on accountability, and has also produced an Accountability Framework to help organisations.[42] Effective and appropriate use of age assurance will be a factor in any decisions that the Commissioner makes around regulatory action relating to the code. It is imperative that organisations can demonstrate this.

4.2 Age assurance and AI

4.2.1 Biometric data

Age assurance may, depending on the type of technology used, involve the processing of biometric data in order to uniquely identify the individual accessing the platform or service. In that case this will be special category data under Article 9.

In these cases, organisations firstly need to identify a lawful basis under Article 6, and then a processing condition under Article 9.

If the use of biometrics is proportionate for age assurance, given the level of risk to children, then it is likely that the following will apply:

- Article 9(2)(g), substantial public interest; and
- Section 10(3) of the DPA 2018 will be met through the "safeguarding of children and of individuals at risk" condition in Schedule 1, Para 18 of the DPA 2018

[41] Controllers, joint controllers and processors | ICO
[42] Accountability and governance | ICO

Organisations must demonstrate why this is the case relative to their specific circumstances according to the general accountability principle. They also need to have an appropriate policy document in place detailing compliance measures and retention policies (Schedule 1 Para 5 of the DPA 2018).

The Commissioner has published detailed guidance about special category data, including the substantial public interest conditions in the DPA 2018.[43]

Beyond biometric data, the specifics of the processing may mean that other special category data is involved. This also needs to satisfy a condition for processing.

4.2.2 Statistical accuracy

In many cases, the output of AI processing amounts to a statistically informed guess rather than a confirmed fact.[44] The algorithm provides an estimate of age within a range, and no algorithm is 100% accurate.

Organisations must ensure that any automated decision-making system is sufficiently statistically accurate and avoids unjustifiable discrimination. This includes systems provided or operated by third parties.[45]

Organisations must decide what their minimum success criteria are for statistical accuracy at the initial business requirements and design phase. They need to bear in mind the risks their service poses to children.

They should test their AI system against these criteria at each stage of the lifecycle. This includes post-deployment monitoring.

Trade-offs may be required in the design of the algorithm. To use a simplified example, there is a balance between precision ('how sure we are that someone has been correctly classified as under 18') and recall ('how sure we are that we have identified all of the under 18s trying to use a platform or service'). Increasing precision means a greater risk of missing some underage users, whereas increasing recall means more adults will be wrongly classified as underage. The correct balance will depend on the exact circumstances, risks and harms identified.[45,46]

4.2.3 Algorithmic bias

An AI algorithm is only as good as the data used to train or tune it.[47,48] There are numerous real-world examples where discriminatory outcomes result from algorithms that are trained on data that does not properly represent the

[43] Special category data | ICO
[44] Accuracy of AI system outputs and performance measures | ICO
[45] What do we need to do to ensure lawfulness, fairness, and transparency in AI systems? | ICO
[46] What is precision and recall in machine learning? - Opinosis Analytics (opinosis-analytics.com)
[47] Ethics, Fairness, and Bias in AI - KDnuggets
[48] A Hidden Trap for CIOs: Data-set Bias in Machine Learning | CIO

population they will be applied to. Usually, the worst effects of such discrimination fall on groups who are already marginalised or vulnerable.

Organisations should ensure that algorithms are trained using high-quality and relevant data sets. The Commissioner's guidance on AI and data protection sets out ways in which developers can mitigate biased, discriminatory or otherwise unfair outcomes resulting from automated decision-making.[49]

Capture bias must also be considered. This is where the device that observes biometric data does so inaccurately. For example, a camera used in poor lighting conditions may produce a photograph of the user that is not of good enough quality for accurate age estimation.

4.3 Age assurance and profiling

Profiling refers to any form of automated processing of personal data that uses the personal data to evaluate certain aspects relating to a person.[50] Information is analysed to classify people into different groups or sectors, using algorithms and machine-learning. This analysis identifies links between different behaviours and characteristics to create profiles for individuals.

Profiling can be used for age assurance (for example, through monitoring aspects of a user's vocabulary and interests to identify potentially under-age users). If this takes place, organisations need to show that it is proportionate to the risks to children that it is being used to mitigate. Profiling data gathered for age assurance must not be used for any incompatible purpose. If profiling for age assurance relies on cookies, such cookies are permissible under the "strictly necessary" exemption.[51]

The Commissioner has published detailed guidance on the rules about cookies and similar technologies.[52]

[49] What do we need to do to ensure lawfulness, fairness, and transparency in AI systems? | ICO
[50] Article 4(4) of the UK GDPR
[51] 12. Profiling | ICO
[52] Cookies and similar technologies | ICO

5. Conclusion and next steps

5.1 Conclusion

Overall, the Commissioner concludes that age assurance is an important tool to enable platforms and services to manage the risks that children face in the online world.

The information and privacy risks that apply to all users of platforms and services online have a greater impact on children. In particular, those associated with profiling and geolocation (which can also put children at risk of physical harm).

The severity of these risks and harms means that the Commissioner has expectations that platforms and services will take the steps necessary to meet the code. Age assurance is a critical component of this, as it enables risk and harm mitigation to be effectively targeted. This is especially the case on platforms that typically cater to a range of ages and where the types of data processing undertaken carry a higher risk of harm to children. Organisations are responsible for assessing risk and potential harm and demonstrating that they have effectively mitigated them. This includes any age assurance process that is in place.

Age assurance involves processing personal data, meaning that:

- the approach used must be based on a thorough assessment of risk, and be proportionate to that risk;
- the approach used must be based on good data protection practice, particularly about transparency, fairness, lawfulness, accuracy, data minimisation and purpose limitation;
- the approach used must be explained clearly to child users, in an age appropriate way and conform with the code standard on transparency;[53] and
- organisations using age assurance must be able to demonstrate that the approach they are using conforms with the code and complies with data protection law.

If organisations do not have a level of certainty about the age of their users that is appropriate to the risks to children, then the alternative is to apply the standards in the code to all users. This should mean that children will still receive some important protections in how their personal data is used. This will be the case even if organisations are unable to confirm the age of their users, or if a child or their parent/guardian has lied about their age. This should be done

[53] 4. Transparency | ICO

in a way that minimises disruption to access by adults and the collection of additional data, and should avoid adding friction to user experience.

Multi-national organisations are required to conform to these standards for the UK and the Commissioner expects to see this being done globally, in order to meet the best interests of children globally.

5.2 Next steps

The data protection risks that the Commissioner outlines in this Opinion feed into some of the most serious online harms that affect children. Age assurance has the potential to be an important part of protecting children from other harms associated with inappropriate content or contact online. This protection is also an essential element of the Best interests of the child.

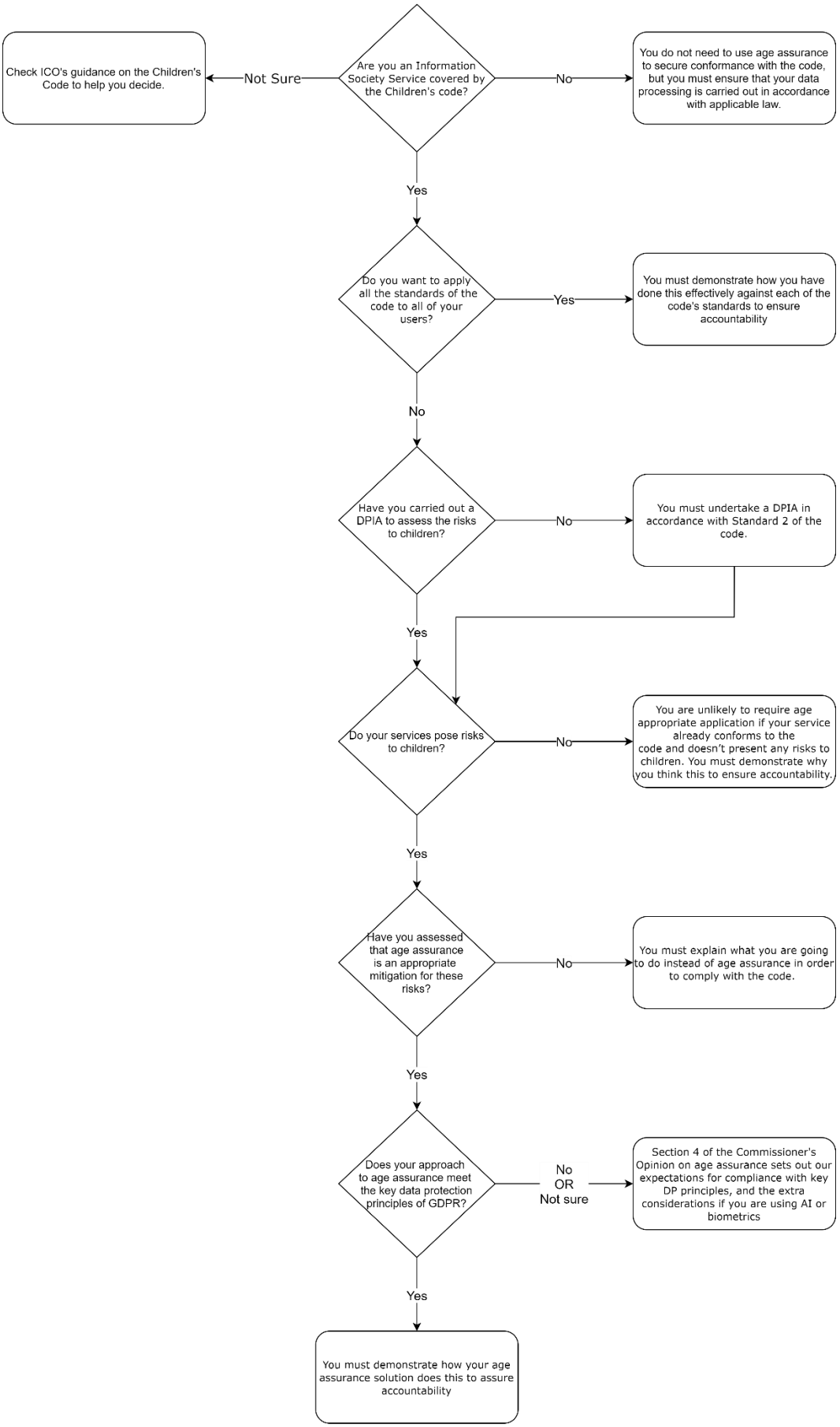
However, these issues will primarily fall within OFCOM's scope given their current role as VSP regulator and future role as online safety regulator. The Commissioner is working closely with Government, the DRCF, and other regulators to ensure a joined-up approach to regulation.[54] Our work with Ofcom will promote a coherent approach to regulation and best practice in age assurance that is compliant with both the privacy requirements in data protection law and relevant legislative requirements to protect children from harmful material online.

The Commissioner will continue to engage with relevant stakeholders, including Ofcom, the Children's Commissioner, Government, and industry, as the understanding of emerging age assurance approaches develops. As part of this, the Commissioner welcomes engagement from interested parties, particularly about evidence of emerging age assurance techniques and their accuracy.

We have launched a call for evidence alongside this opinion and we will continue to develop our approach to age assurance as new technology emerges and the market evolves.

[54] Digital Regulation Cooperation Forum | ICO

Annex 1: Age assurance flow chart



Annex 2: Current uses of age assurance

Age verification

Age verification is primarily used by sites that provide goods or services that attract criminal or civil penalties for serving underage customers:

- online retailers who sell age-restricted products, for example alcohol, tobacco products including vape, and knives. There are 56 products subject to such restrictions in UK law; and
- providers of age-restricted services such as gambling.

In these instances, the use of disclaimers by the provider, or reliance on user confirmation of age, is insufficient to comply with the law. Reliance on the user confirming publicly available or easily discoverable data such as date of birth is also insufficient.

Verification is carried out through documentation, such as a passport, or credit reference checks. For example, where an individual holds a credit card, this may be used as a proxy indicator of age, since credit cards are restricted to people over the age of 18.

There is a risk of excluding or indirectly discriminating against individuals who lack the necessary documentation or data, such as credit history. Organisations should therefore take a holistic approach to what hard identifiers they accept. Organisations should also take the Equality Act into account and the requirement to ensure reasonable adjustments for those with protected characteristics. For example, they may wish to consider accepting a broad range of hard identifiers such as a GP letter, a utility bill or letter from a social worker or social housing provider, rather than only relying on passports, driving licences or credit cards.

Age assurance services are frequently provided to platforms or services by third parties. An advantage of third-party age assurance services is that they can, depending on the approach taken, provide an age assurance decision without the third party needing to provide the data controller with additional personal data about the subject.

Most age verification services cannot be readily used to determine the age of a child as they only provide confirmation that the data subject is over or under 18. It is not a solution for age-appropriate design elements such as tailored transparency or nudging. Age verification could be used to determine age based on documentation, but this would be highly intrusive.

We recommend that an appropriately certified supplier is used, or that ISS carrying out their own age verification certify the process that they use. For example, the Age Check Certification Scheme (ACCS) provides an independent check that providers meet the current industry standard, PAS 1296:2018.

Account confirmation

Many platforms and services offer the option to have linked or family accounts. This means that there is a main account holder but additional profiles are set up for other users, such as children. As part of this, linked or family accounts can be used to confirm the age of an account or profile user with the main account holder.

This is a useful way of enabling children access to an age appropriate version of a service, whilst ensuring there is parental control. It can be effective, particularly when different aspects of a service are aimed at different age groups, and users include a mix of adults and children. However, it relies on the parents or guardians being able and willing to actively set up different profiles and confirm each profile user's age. It also depends on the level of certainty that the person overseeing the child's access is genuinely the parent or legal guardian. There is a risk that they are not providing an accurate age for the child in order to allow them access to a service.

Where the risks of the service are high, we expect a high degree of certainty that the person verifying and controlling the account is an appropriate adult. This may also require the use of age verification solutions.

Children have the same rights as adults under UK GDPR.[55] Even if a child is too young to understand the implications of their rights, they are still their rights, rather than anyone else's such as a parent or guardian. You should therefore only allow parents to exercise these rights on behalf of a child if:

- the child authorises them to do so;
- the child does not have sufficient understanding to exercise the rights themselves; or
- it is evident that this is in the best interests of the child.

This applies in all circumstances. This includes in an online context where the original consent for processing was given by the person with parental responsibility rather than the child.

The Commissioner has published guidance on children's information rights.[56]

Age estimation

Our engagement with industry so far suggests that age estimation products using a mix of biometric data, profiling and other information will become commercially available on a relatively short timescale. These include:

[55] In Scotland there is a presumption that a child of 12 or over has sufficient understanding to be able to exercise their rights. In England and Wales there is no presumption, but it forms a useful guideline.
[56] What rights do children have? | ICO

- using computer vision-based approaches to estimate age from an image of the subject. The image may be captured in real time by the user's mobile device camera or webcam. Some approaches additionally compare the real-time image to one from an accepted form of photographic ID to provide additional confirmation;
- using data derived from images such as facial geometry to make a similar determination; and
- analysing profiling data derived from the user's activity on social media and other platforms.

A number of other techniques are occasionally mentioned in academic literature and specialist press, but have yet to make notable progress towards commercial availability, including:

- voice analysis;
- hand geometry;
- Natural Language Processing (NLP); and
- behavioural analysis (this can also be applied to existing users, eg to detect a malicious actor attempting to impersonate a child, or a child attempting to impersonate an adult). Social media platforms may be well placed to develop these approaches given their existing profiling capabilities.

Age estimation techniques generally use Artificial Intelligence (AI) algorithms to automate the interpretation of data. There is little evidence for the effectiveness and accuracy of these emerging approaches. It is likely that implementation of the Children's code, coupled with upcoming legislation that aims to tackle online harms will help to stimulate the market and encourage further research and development.[57]

[57] Guidance on AI and data protection | ICO

Annex 3: Economic Impact of Age Assurance

The impact of age assurance is potentially far-reaching but in the interests of a proportionate assessment, we focus on:

- ISS Providers;
- data subjects;
- age assurance providers; and
- the ICO.

The following table provides an overview of potential impacts that might arise for each of the affected groups. This is not an exhaustive list but covers those we perceive to have the highest likelihood and potential severity. This represents our understanding at the time of publication and we will continue to develop our analysis over time.

ISS or Age Assurance Providers	Data subjects	ICO	Wider/ Societal
Positive Impacts (Benefits)			
• Greater degree of regulatory certainty. • Levels the playing field for providers that are already compliant. • Easier to demonstrate accountability and compliance to customers/end users and other stakeholders • The opinion may obviate the need for controllers to seek specific legal advice on the matter and hence reduce costs. • Reduced potential to be subject to regulatory action by the ICO if the opinion is followed. • Parents, guardians, carers and children may feel more confident about	• Improved safety for children online and reduction in harms associated with accessing inappropriate materials and services. • Potential for better targeted services resulting in an enhanced online experience for both adults and children. • Potential for better protection of the personal data collected for age assurance through data minimisation.	• The ICO will be in a better position to assess compliance and take appropriate regulatory action where required. • The ICO's reputation could be enhanced by being seen to take action in a particularly sensitive area. • Providing guidance within the opinion may help mitigate the burden of regulatory action later. • Less likelihood of complaints from members of the public.	• Potential for increase innovation activity in age assurance and related technologies. • Increased demand for age assurance technology supply chain. • Reduction in the societal harms arising from poor protection of children online such as increased crime and poor educational attainment. • Could help to realise some of the government policy objectives of the online safety bill. • Potential for societal benefits from the improvement of efficiency and effectiveness of public

ISS or Age Assurance Providers	Data subjects	ICO	Wider/ Societal
using products and services, increasing demand and/or revenue for organisations. • Easier to target services appropriately as adults will be easier to distinguish from children online. • Increased demand for services from compliant age assurance providers and technology developers.			services that rely directly or indirectly on age assurance.
Negative Impacts (Costs)			
• Compliance costs, which include familiarisation costs, may increase (eg reviewing the opinion, seeking legal advice, amending services, implementing new age	• Individuals may be restricted from using products and services that they currently use. • Services could become more expensive or less effective.	• Potential for the ICO to be perceived as creating barriers to competition or innovation in certain sectors. • Potential for the ICO to be perceived as not going	• Potential for regulatory overlap, depending on the final draft of the Online Safety Bill or resulting secondary legislation or codes leading to uncertainty for

ISS or Age Assurance Providers	Data subjects	ICO	Wider/ Societal
assurance measures etc). • Potential for some activities to be restricted or made no longer viable by the opinion, leading to reduced revenues. • Age assurance providers and technology providers of technologies that are now deemed non-compliant or higher risk may see reduced demand and revenues. • Public authorities could become unable to effectively provide services.	• Individuals may be required to go through additional steps (eg submission of evidence, lengthier Ts and Cs or additional tick boxes)	far enough to protect children online. • The ICO could be subject to legal challenge from ISS or age assurance providers, or civil society groups that believe the opinion doesn't go far enough.	providers and data subjects. • Potential reduced demand or revenue for ISS or age assurance provider supply chains.