SLAUGHTER AND MAY

21 July 2026

Beyond the OSA / DSA: Age Assurance as a Data Privacy Obligation

A version of this briefing first appeared in the Privacy Laws & Business UK Report, Issue 146 (July 2026).

The need for age assurance has been much discussed in the context of the EU Digital Services Act (DSA) and the UK Online Safety Act (OSA) and the organisations to which they apply, and even more so in light of the UK Government's announcement of a social media ban for under 16s. However, there has been less attention on the need for a much broader range of websites and apps to introduce age assurance in order to comply with their obligations under the GDPR. Most of the discussion from a privacy perspective has instead related to the need for age assurance technologies themselves to comply with privacy laws. This is of course important, but it has camouflaged the wider point that privacy laws themselves may mean that age assurance is required in order for the website/app to be GDPR compliant, regardless of the position under the OSA or DSA.

UK data privacy laws apply to all organisations, compared to the much narrower application of the OSA / DSA regimes. A much larger spectrum of organisations therefore need to take note of the developments on age assurance than may currently realise it, including retailers of fashion, beauty or sports, toys or games which are either online or collect personal data in store, events and entertainment ticket sellers and sports clubs and teams. These, and other businesses, need to (re)assess what personal data they are collecting and whether or not they are required to implement age assurance for GDPR reasons.

This is nothing new - the Children's Code has always referred to age assurance

The ICO has long been focused on protecting children online, with the UK's Age Appropriate Design Code (known as the Children's Code) taking effect in 2021. It applies to services 'likely to be accessed by' children (i.e. under-18s). As a statutory code, the Children's Code has a greater impact than ICO guidance more generally, as in any court proceedings the court is obliged to take its provisions into account.

What is age assurance?

Age assurance is the process of establishing, determining and/or confirming either an age or an age range of a natural person. It is an umbrella term encompassing all methods that help estimate or assess a user's age and therefore allows providers to tailor user experience to the user's age, or to enforce age-appropriate access restrictions, where legally required.

The Code sets out 12 standards to follow, with the most pertinent in the context of age assurance being Standard 3:

"Age Appropriate Application: Take a risk-based approach to recognising the age of individual users and ensure you 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."

So, why the increased focus from the ICO now?

At a conference in June, the ICO confirmed children's processing has always been a priority, but that the risks are heightened by developments in AI. In addition, the ICO's approach has tended to be focused on education and engagement before enforcement, often with a certain amount of pragmatism on the challenges that are beyond businesses' control. Hence it was important for the Children's Code to be bedded in first before the ICO turned to potential enforcement action.

The Children's Code is non-prescriptive about what methods should be used to establish age and specifically

notes that new methods may emerge over time. The ICO also acknowledged in its 2024 Age Assurance Opinion that the age assurance market is developing rapidly and cautions that, when assessing compliance, it will take into account products available at the relevant time. This development of new, better technology therefore in large part explains recent focus from the ICO on age assurance, as businesses have less of an 'excuse' for not complying.

The other potential factor, aside from public focus and political emphasis on children's online safety, is that the Data (Use and Access) Act 2025 introduced a new requirement for online services likely to be accessed by children to consider the protection of children in designing and operating their services. The ICO has recognised that organisations already complying with the Children's Code will satisfy this so, in effect, the new requirement bolsters the importance of the Children's Code as opposed to changing anything per se. However, given this requirement came into force in February this year, it arguably also helps to explain the ICO's invigorated focus on age assurance in recent months.

The death of self-declaration

In its open letter to social media and video sharing platforms in March, the ICO recognised that to date most services have relied upon self-declaration, but that the "status quo is not working". The ICO points to the fact that there are now "new viable and privacy friendly solutions" because age assurance technologies have advanced rapidly in recent years, and calls on the services to implement effective age gates using the new technologies.

Although the ICO's comments in the open letter are directed to the addressees, their message has broader implications – organisations relying on self-declaration need to reconsider whether to introduce other age assurance solutions, unless their processing poses only low-level risk to children.

Website terms are ineffective by themselves from a privacy perspective

Merely stating in website terms and conditions that the website is not intended for children and that they may only access it with parental consent is also unlikely to be sufficient from a privacy perspective. This was emphasised in the ICO's fines against Reddit and Imgur earlier this year (discussed in this blog), as a key failure in both cases was that they relied on a restriction in their terms and conditions, with the ICO determining that this was insufficient to prevent children accessing a service without other measures being in place, such as an effective age assurance mechanism.

Age restriction in website terms must be enforced

Not only is an age restriction in terms and conditions insufficient to demonstrate age assurance, the joint statement by the ICO and Ofcom on Age Assurance (the "Joint Age Assurance Statement"), published in March, states that where there is such a term, age assurance will be required in order to be GDPR compliant as the organisation will generally have no lawful basis for processing the personal data of children who are not meant to be on the site or app in the first place.

Given it is commonplace to include an age restriction in terms and conditions, organisations should review whether this is actually necessary for their services by reassessing whether children are likely to access their site/app. If so, and the organisation does not want children to access the site/app, the organisation should consider what the most appropriate age assurance mechanism would be to enforce this.

Alternatively, if it is concluded that children are not likely to access their site/app, organisations may prefer to remove the age restriction entirely to avoid the risk of not having a lawful basis for processing the personal data of any children who do in fact access their site or app. For instance, children are unlikely to access a website about pension products, so why include a restriction in the website terms saying they may not do so? Of course, there may be other, non-UK privacy related reasons for the age restriction such as the sale and/or marketing of age restricted products or under the laws of other jurisdictions, so this will need to be considered before any change is made.

When age profiling can be used

The ICO noted in its Children's Code Strategy update in December last year that profiling is sometimes used in place of, or to supplement, self-declaration by inferring or estimating age. Following input from four organisations who used age profiling, the ICO concluded that profiling has a place in the range of age assurance measures as an anti-circumvention tool to identify those under the permitted age who have slipped through robust age gates.

However, the ICO concluded that it is not appropriate to use profiling to make up for a weak or non-existent age gate if those under a specified age are not permitted on a service. In addition, given profiling requires a user to already be on a service in order to infer an age based on their activity, services which have a minimum age risk unlawful processing if they solely rely on age profiling. This is because the service will process the personal information of children who are not meant to be on it before the profiling is able to provide an age inference.

How to implement privacy-compliant age assurance?

The more sophisticated age assurance technologies collect more data about the individual and so come with their own data protection risks that need to be carefully managed.

Whilst the Joint Age Assurance Statement was aimed at services in scope of the OSA, it is relevant more broadly to organisations implementing age assurance technologies, for instance to prevent marketing to children. The statement expressly recognises that all age assurance methods involve the processing of personal data and that organisations can process personal data for age assurance provided that the age assurance method chosen is necessary, effective for the purpose and proportionate to the level of risk of the relevant service.

Different types of age assurance technology pose distinct risks. For example, some types, such as Digital IDs, that rely on initial verification via an official ID (such as a passport), can contribute to exclusion as some socio-economic groups are less likely to have the relevant ID, whilst age estimation relies on the collection of sensitive, special category and biometric data, and may also introduce different risks of algorithmic bias against certain ethnic groups. Whichever method is chosen, its particular risks must be evaluated and the processing must comply with GDPR data protection principles.

When selecting an age assurance technology, organisations should therefore consider the following key areas.

- Fairness and accuracy: age assurance solutions must be adequately and consistently accurate, and risks of bias need to be scrutinised and mitigated, as verified through testing and supplier due diligence. Users must have accessible means to challenge decisions.
- Transparency: users must receive clear, age-appropriate information about the methods used, the rationale and the personal data processed. Concise "just in time" explanations should be provided at the point of interaction, and prompts enabling children to choose whether to proceed may be appropriate in some cases.
- Minimisation: alternatives to inspecting official ID documents, such as the use of selective disclosure from Digital IDs or on-device processing, should be used to reduce personal data collected. Data retention should be limited, for example storing only pass/fail outcomes rather than user ages.
- Security: robust supplier due diligence and contractual safeguards must address breach detection, reporting, remediation and service disruptions. Transparency materials should be reviewed to ensure they do not expose vulnerabilities to malicious actors.

The ICO has developed a certification scheme for age assurance services, providing independent assurance that a provider meets data protection requirements. Organisations should consider whether a prospective provider holds ICO certification as a factor in their selection process, as this can support accountability and demonstrate compliance with the UK GDPR and the Children's Code.

In addition, the UK Government announced on 15 June that Ofcom will assess what amounts to highly effective age assurance for determining if someone is 16 or over, without excluding users who lack the means to verify their age through passports or driving licences. The announcement specifically calls out the importance of data privacy and security in Ofcom's assessment. Ofcom is due to report by October.

Potential for enforcement?

In line with its fines against Reddit and Imgur, the ICO has stated that those websites and apps which continue to rely primarily on self-declaration will be a key focus in its work this year, with the regulator having identified 17 high-risk platforms which it believes do so. Earlier this year the ICO wrote to TikTok, Snapchat, Facebook, Instagram, YouTube and X asking them urgently to review and strengthen age assurance. However, none of them have yet introduced new, viable and privacy-friendly age assurance solutions,

according to an ICO statement in May (discussed in this blog). In its response to the Government's social media consultation, the ICO has indicated that regulatory action may be required where social media companies are disputing the ICO's findings rather than making changes. It has called for the Government to facilitate "more efficient regulatory outcomes" in this area by streamlining the data protection appeals process.

Also in May, Ofcom flagged to the UK Government that the OSA does not explicitly require services within its scope to keep underage children off their platforms by using robust age checks. As things stand, any enforcement action for age assurance failings therefore needs to be brought by the ICO for GDPR non-compliance, whether or not the organisation falls within the OSA's scope. This is unlikely to be the case for long however, as in its 15 June announcement, the Government called for an urgent review of Ofcom's enforcement capabilities, which suggests that Ofcom's powers may soon be bolstered in this space.

Practical steps for organisations to take

- Reassess, and document, whether children are likely to access your websites/apps. This will need to be kept under review if the nature of your business evolves in such a way that would impact the likelihood of children accessing them.
- Check whether your website/app terms include an age restriction, assess on what basis the requirement is included and determine whether it continues to be required.
- Where relevant, assess the most appropriate age assurance mechanism to introduce to balance the risk of the additional processing of personal data versus the risks to children posed by having their personal data processed on your websites/apps. This will need to be kept under review as technologies and regulatory expectations evolve.
- Complete a data protection impact assessment (DPIA) for any age assurance mechanism that is implemented, having regard to standard 2 of the Children's Code, which provides guidance on DPIAs tailored to address risks to children. As with all DPIAs, this should be reviewed and updated as necessary at appropriate intervals.

Looking ahead

The ICO's current focus on social media and video sharing platforms aligns with its general position to focus on areas where it assesses there to be the greatest privacy risks and reflects the public and media attention these platforms are receiving. However, other organisations should not take this to mean that they will not be within the ICO's sights in the next wave and so would do well to take proactive action now.

Contact

Rebecca Cousin
Head of Data Privacy
T: +44 (0)20 7090 3049
E: rebecca.cousin@slaughterandmay.com

Bryony Bacon
Senior Knowledge Lawyer
T: +44 (0)20 7090 3512
E: bryony.bacon@slaughterandmay.com

Cindy Knott
Head of Data Privacy Knowledge
T: +44 (0)20 7090 5168
E: cindy.knott@slaughterandmay.com

London
T +44 (0)20 7600 1200
F +44 (0)20 7090 5000

Brussels
T +32 (0)2 737 94 00
F +32 (0)2 737 94 01

Hong Kong
T +852 2521 0551
F +852 2845 2125

Beijing
T +86 10 5965 0600
F +86 10 5965 0650