European Commission

Analysis of the impact of age assurance on fundamental rights and the financial impact on businesses concerned

Follow-up to the recommendations of the co-chairs of the Special Panel on child safety online

Written by Owen Bennett
October 2026

EUROPEAN COMMISSION

Directorate-General for Communications Networks, Content and Technology
Directorate F — Online Platforms: Society
Unit F3 — DSA Protection of Minors and other Societal Risks

European Commission
B-1049 Brussels

Analysis of the impact of age assurance on fundamental rights and the financial impact on businesses concerned

Follow-up to the recommendations of the co-chairs of the Special Panel on child safety online

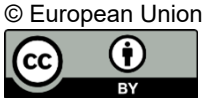
Directorate-General for Communications Networks, Content and Technology

2026

The information and views set out in this report are those of the author and do not necessarily reflect the official opinion of the Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein. Any final decision taken on the basis of the analysis prepared by the contractor will be the result of an independent assessment by the Commission services.

PDF ISBN 978-92-68-44492-4 doi: 10.2759/8990450 KK-01-26-173-EN-N

© European Union, 2026



The Commission's reuse policy is implemented by Commission Decision 2011/833/EU of 12 December 2011 on the reuse of Commission documents (OJ L 330, 14.12.2011, p. 39 – https://eur-lex.europa.eu/eli/dec/2011/833/oj).

Unless otherwise noted (e.g. in individual copyright notices), the reuse of this document is authorised under the Creative Commons Attribution 4.0 International (CC BY 4.0) licence (https://creativecommons.org/licenses/by/4.0/). This means that reuse is allowed, provided appropriate credit is given and any changes are indicated.

Contents

Abstract **6**

Executive Summary **7**

1. Introduction **14**

1.1. Purpose of this report 14

1.2. The context for age assurance 15

1.3. Structure of the report 17

2. Fundamental rights impact **19**

2.1. Data protection and privacy 19

2.1.1. Mapping the rights interference 19
2.1.2. How can it be mitigated? 21
2.1.3. Conclusion and summary of recommendations 27

2.2. Non-discrimination 28

2.2.1. Mapping the rights interference 28
2.2.2. How can it be mitigated? 30
2.2.3. Conclusion and summary of recommendations 35

2.3. Freedom of expression and access to information 36

2.3.1. Mapping the rights interference 36
2.3.2. How can it be mitigated? 39
2.3.3. Conclusion and summary of recommendations 45

3. Financial impact **46**

3.1. Deployment costs 46

3.2. Ongoing costs 49

3.3. Longer term economic projection 53

3.4. Impact on SMEs 55

3.5. Conclusion and summary of recommendations 57

4. Conclusion **59**

Abstract

The final report of the Special Panel on child safety online recommended that the EU introduce fundamental rights-respecting age assurance requirements to better protect children online. Building on that work, this report examines how rights-respecting age assurance could be operationalised in a future EU legislative instrument. It analyses interferences with the three fundamental rights most directly engaged by the practical deployment of age assurance: the rights to data protection and privacy, to non-discrimination, and to freedom of expression and access to information. It argues that these interferences could be substantially mitigated through, inter alia, strict enforcement of the GDPR, the leveraging of privacy-preserving deployment architectures, and a focus on choice and optionality. The report also analyses the likely financial implications of an age assurance mandate for in-scope service providers, finding that while online services would invariably face novel costs, these would likely be modest for most services and would fall over time. Finally, it finds that the EU Age Verification blueprint can make an important contribution to a future legislative instrument as a privacy-preserving and likely low-cost means of operationalising age assurance, provided Member States first close the existing deployment gap.

Executive Summary

Introduction

In their final report to European Commission President von der Leyen in July 2026, the co-chairs of the Special Panel on child safety online recommended that the EU introduce fundamental rights-respecting age assurance requirements to protect children online.

As European Commission DG CNECT reflects on the recommendations of the Special Panel, this report engages with the critical question of how precisely age assurance can be implemented in a manner that is rights-respecting. It separately explores the financial impacts of a future legislative instrument, for the service providers who would likely be required to deploy age assurance.

The context for age assurance in the EU

Age assurance has become an increasingly prevalent feature of the online sphere in the EU in recent years, for both adults and children who use web services, and for the economic operators who offer them.

EU-based web users seeking to purchase age-restricted goods like alcohol or partake in age-restricted activities like gambling, will normally encounter an age check requiring them to assure that they meet the relevant age threshold. Likewise, as online and offline worlds become increasingly inseparable, age (and age assurance) has become an ever-more important factor through which operators of online services – of their own volition – shape *who* can access their service and under *what* conditions.

While support among broader stakeholders is far from universal, there is emerging *political* consensus on the proportionality of age assurance as a policy approach, when it is undertaken in a manner that is rights-respecting. The Special Panel's recommendations on age assurance echo similar calls from legislatures including the European Parliament, regulatory networks including the European Data Protection Board, and multilateral institutions including the Council of Europe.

At the same time, the age assurance sector is expanding and evolving rapidly, both in terms of commercial offerings and technological innovation. Standards development organisations and conformity assessment bodies have begun to establish criteria for how providers should operate and how their solutions should function, while market demand is incentivising age assurance providers to increasingly compete on privacy, usability, and deployment ease.

Taken together, age assurance – in the manifold forms it takes – is becoming an ever-more common feature of experiencing and of offering online services in the EU today.

Rights interferences

This report focuses on the three fundamental rights most directly engaged by the deployment of age assurance. These are the rights to data protection and privacy, the right to non-discrimination, and the right to freedom of expression and access to information. It is beyond the scope of this report to treat fundamental rights questions that arise *prior* to the practical deployment of age assurance (e.g. whether age-based restrictions are compatible with the right to freedom of expression and access to information *per se*).

The attributes of a rights-respecting and effective age assurance system – such as accuracy, reliability, privacy, and inclusivity – cannot always be maximised simultaneously. Depending on how the legislator weighs these attributes against one another, a future legislative instrument might prescribe one or more specific methods and assurance levels for certain services or use cases. Alternatively, or for other services and use cases, it could set a general, outcomes-based mandate under which service providers can choose from a variety of methods to satisfy the age assurance regulatory requirement. The nature of the rights interferences, and the necessary mitigations, differ between these two regulatory scenarios, and the report distinguishes between them where relevant.

Data protection and privacy

Age assurance necessarily involves an interference with the rights to data protection and privacy – an individual's age cannot be assured without the collection of *some* personal data pertaining to that individual. The character of these interferences can vary, depending on the chosen method and deployment model of age assurance.

Serious interferences and harm to adults and children can arise out of, amongst other factors:

- excessive data collection in the age assurance process;
- breaches of the personal data that is collected and processed by age assurance providers; and,
- exploitation of the age assurance process by service providers or other third parties for the purposes of commercial profiling.

As is elaborated in the report, there are clear avenues available to the European Commission to mitigate these interferences. In a future legislative instrument the European Commission should:

1. **Ensure legislative coherence with the GDPR**. Ensure that data protection authorities in the EU are **properly resourced** to apply the GDPR principles and protections to age assurance deployments and service providers.
2. Ensure age assurance methods and deployment models that are permissible under a future legislative instrument meet **high standards of**

privacy and security, in terms of their product policies, system architectures, and technical approaches (e.g. through the use of double-blind architectures).

3. Encourage – and possibly incentivise – the development and adoption of **technical standards** that establish privacy and security baselines for the age assurance sector.

Non-discrimination

The deployment of age assurance brings foreseeable risks of discrimination and exclusion.

For instance, digital identity-based solutions – including the EU Age Verification blueprint – can discriminate against individuals who do not possess qualifying hard identifiers (like biometric passports), or smartphones with near field communication capability. Facial age estimation (FAE) systems, for their part, create risks of algorithmic bias, amongst other risks.

The report outlines the steps that European Commission should take to mitigate serious interferences with the right to non-discrimination, and to ensure inclusivity. These include:

1. Ensure that EU Member States **provide and adequately resource effective fallback enrolment routes** – including manual enrolment at national and local level, acceptance of a broader range of identity documents, and acceptance of proof-of-age attestations from a broader range of trusted sources. This will help ensure that individuals who lack qualifying chip-based hard identifiers, or who do not have access to an NFC-capable smartphone, are not precluded from using EU Age Verification blueprint-based solutions.
2. Consider developing **secondary legislation that elaborates the non-discrimination principles of the Article 28 Guidelines, or consider leveraging standards like ISO/IEC 27566-1**, to bring greater transparency, direction, and accountability to how age assurance providers and deployment models ensure non-discrimination.
3. Where a specific assurance method and level is not prescribed for compliance, ensure **choice and optionality** in the age assurance process. Specifically: encourage or require that service providers offer a plurality of distinct age assurance methods, with fallback when the preferred method fails.
4. Irrespective of the method deployed, ensure that online services make provision for escalation and **user support channels.**

Freedom of expression and access to information

Arguably the most prominent interference of age assurance with the right to freedom of expression is the restriction that it places on children's ability to engage with certain types of online spaces and certain forms of online content.

Interferences that arise when age assurance is being *deployed* – the focus of this report – are direct and experiential as well as diffuse and perceptual. In terms of interferences that arise in the experience of age assurance, the reality of having to assure their age more frequently might dissuade some of-age individuals from using online services or, if they are unable to assure their age using the available methods, might lead to them being locked out of services. Furthermore, public suspicion that an age assurance mandate is the first step towards generalised online identification and surveillance infrastructure might likewise push of-age users away from online services, or engender a chilling effect in how they express themselves and seek information online.

To address these and related concerns, the Commission should, in any future legislative instrument:

1. **Ensure friction is minimised and choice is optimised in adults' and children's experience of the age assurance process.** Where no specific method is prescribed, this can be done by requiring or incentivising multiple age assurance methods and permitting successive validation-style deployments; where a specific method is prescribed, by ensuring choice of onboarding routes, attestation issuers and providers within that method; and in all cases, by encouraging interoperability and reusability of age checks.
2. **Prioritise meaningful communication and clear transparency** to adults and children, both at the regulatory implementation stage and during the practical user experience flow.
3. Build the regulatory framework around technologies and deployment models capable of being **privacy-preserving,** and ensure **strict compliance with the GDPR** throughout.

Financial impact

A requirement to implement age assurance in the EU will invariably introduce novel costs for the service providers subject to it.

Precise estimation of the sector-level economic impact of age assurance requirements is constrained by a lack of rigorous existing quantitative data. However, the experience of jurisdictions like Australia and the UK – where broadly scoped age assurance requirements are already in place – provides useful insight into the cost implications for service providers. Self-reported vendor data also helps illuminate the cost environment that would likely be faced by in-scope services.

Deployment costs

In response to a legislative requirement for age assurance, most services would likely deploy third-party solutions, whether the EU Age Verification blueprint or one of the many offerings available from the wider age assurance sector.

The age assurance sector is increasingly competing on ease of integration, with vendors advertising integration timelines of days or less, and offering ready-made plugins for common website builder platforms like Shopify and WordPress.

Deployment costs should therefore be low for the great majority of services, and cluster around the hundreds of euro or the low thousands. Service providers that seek to build and deploy proprietary in-house age assurance systems would incur far higher costs – likely in the hundreds of thousands of euro.

Ongoing costs

Service providers' ongoing costs associated with age assurance bifurcate into operational costs and per-check costs.

Operational costs, such as compliance, information security, and user support, will likely scale in proportion to the number of age checks that a service provider performs. Reliance on third-party age assurance solutions that bundle these services, or the leveraging of existing corporate capabilities in functions such as information security and user support, could meaningfully ease the increased cost burden.

Per-check costs, by contrast, are typically inversely related to the volume of checks performed, meaning the marginal cost of each check tends to fall as the volume of checks rises. While costs vary depending on the method used, implementation data regarding the UK age assurance mandate estimates that the per-check cost incurred by services has a median of around EUR 0.07, with most checks falling at or below a cost of EUR 0.12.

Longer term economic projection

Service providers' costs for age assurance are likely to trend downwards over the medium term. In particular, services should see benefit from:

- the continued technological and commercial advancement in how age assurance is developed and deployed;
- the growing maturity of mutual recognition initiatives, which mean the cost of age assurance can be shared across participating service providers; and,
- the spread of age assurance regulatory mandates globally, which allows service providers to amortise costs across a larger operational base.

Impact on SMEs

A future legislative instrument will invariably introduce novel costs for small-, and medium-sized enterprises, costs which might be proportionally higher than those faced by larger players.

SMEs are, however, likely to be substantially insulated from excessive costs. This is because of the availability of low-cost solutions like the blueprint, sustained competition among vendors for easy-to-deploy solutions aimed specifically at smaller providers, and the harmonising effects of an EU-level instrument, compared with the patchwork of fragmented Member State requirements.

Recommendations for implementation

Ultimately, while increased costs for service providers will invariably follow from a requirement to implement age assurance, the European Commission can alleviate service providers' costs through the following actions:

1. **Accelerate the roll-out of the EU Age Verification blueprint across all Member States.** The blueprint's publicly funded, open-source architecture gives it the potential to be among the cheapest available compliance pathways for service providers of every size, including on a per-check basis.
2. **Permit and encourage deployment approaches that reduce friction and per-check costs**, such as successive validation (when no specific method is prescribed), reusable proof-of-age attestations, and interoperability.
3. **Develop secondary legislation and/or leverage the growth of technical standards for the third-party age assurance sector,** to reduce costs associated with vendor due diligence for service providers.

The role of the EU Age Verification blueprint

The EU Age Verification blueprint can make an important contribution to the emergence of a coherent, EU-level approach to age assurance.

It is privacy-preserving and open by design, and because its development costs have been publicly subsidised, it is likely to amount to a low-cost means of complying with age assurance requirements for service providers of every size.

However, there is currently a deployment gap. Only a small number of EU Member States today offer a blueprint-based age assurance solution and most Member States lack the supporting infrastructure that is necessary for broad-based use of blueprint-based solutions (e.g. adequately resourced manual enrolment facilities). This deployment gap must be treated as a priority, and addressed before any future legislative instrument on age assurance would enter into force.

Conclusion

The co-chairs of the Special Panel issued a call to action for privacy-preserving age assurance at scale.

That outcome can by no means be assumed. As this report has shown, age assurance poses interferences with the fundamental rights to privacy, data protection, and freedom of expression, and carries foreseeable risks of discrimination and exclusion. In terms of scalability, it also creates novel costs and compliance burdens for service providers, large and small alike.

Yet, as this report has articulated throughout, the deployment challenges associated with age assurance can be substantially mitigated through deliberate legislative design and policy implementation, such as by leveraging privacy-preserving technologies and by facilitating choice – of methods, of onboarding routes, or of providers.

Ultimately, should it decide to introduce dedicated age assurance requirements in the EU, there is a clear path by which the European Commission can make age assurance rights-respecting and proportionate in its deployment.

1. Introduction

In their final report to European Commission President von der Leyen in July 2026, the co-chairs of the Special Panel on child safety online recommended that the EU introduce fundamental rights-respecting age assurance requirements for certain information society service providers[1] [2].

The *Child Safety Online: Protecting and Empowering Minors in a Digital World* report sets out the essential conditions for an EU approach to age assurance to be fundamental rights-respecting, including, for instance, that it upholds the highest privacy and data protection standards and protects against discriminatory outcomes. The report provides further recommendations on the essential *attributes* of a rights-respecting age assurance deployment method, including, for instance, that it functions with a high degree of accuracy and that it utilises state of the art security technologies to safeguard children's and adults' personal data.

1.1. Purpose of this report

As the European Commission Directorate-General of Communications Networks, Content & Technology (DG CNECT) continues its reflections on the Special Panel's recommendations, this report aims to clarify how the co-chairs' vision for rights-respecting age assurance can be operationalised in a future EU-level legislative instrument.

To that end, it will interrogate the fundamental rights interferences that age assurance requirements can engender. Where problematic interferences are identified, the report will offer recommendations for how DG CNECT can mitigate them in a future legislative instrument. In its analysis of interferences and mitigations, the report will engage directly with the systems and technologies that determine how age assurance affects and is experienced by children and adults. The report will treat implications arising from how age assurance is *deployed*, and

[1] Fegert, J., Melchior, M., (2026) Child safety online: *Protecting and empowering minors in a digital world*. Available at: https://commission.europa.eu/document/download/d833504d-5ec3-4fac-945f-38e7d0bd5326_en?filename=Special-panel-report.pdf

[2] Throughout this report, 'age assurance' is used as an umbrella term for the methods and processes used to determine, with varying degrees of certainty, an individual's age or age range. In the few places where the terms 'age verification' and 'age estimation' are used, they are used within the meaning of the European Commission's DSA Article 28 Guidelines. See: European Commission (2025) *Communication from the Commission – Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28(4) of Regulation (EU) 2022/2065, OJ C, C/2025/5519, 10.10.2025*, s. 6.1.4 ELI: http://data.europa.eu/eli/C/2025/5519/oj

it will not engage the prior question of whether mandating age assurance to protect children online is a proportionate policy approach.

The Special Panel's report also calls for an EU-level approach to age assurance that is proportionate and contributory to the proper functioning of the EU Single Market. As consideration of economic and competitiveness matters was beyond the scope of the Special Panel's work, this report will directly probe the likely impact of an EU-level age assurance mandate on the information society service providers who could be subject to such a requirement. It will provide recommendations for DG CNECT as to how those impacts can be managed, taking account of the EU Age Verification blueprint, the state of the age assurance market, and lessons learned from other jurisdictions where companies face similar requirements to deploy age assurance systems. Consideration will be given to the unique situation of micro-, small-, and medium-sized enterprises, and how they can be insulated from excessive cost burdens.

Ultimately, this report will illustrate that while age assurance mandates and practices pose undeniable fundamental rights interferences for children and adults and place novel costs on information society service providers, there are clear and viable means by which the EU legislator can mitigate those rights interferences and alleviate those costs in a future legislative instrument.

1.2. The context for age assurance

Age assurance has become an increasingly prevalent feature of children's and adults' online experience in the EU in recent years.

Individuals who have ever sought to buy age-restricted goods online, such as alcohol or tobacco, or partake in age-restricted practices online like gambling, will invariably have been required to demonstrate that they surpass the relevant age restriction that protects against age-inappropriate access to those goods or services.

Likewise, as online and offline worlds become increasingly inseparable, age and age assurance have become an ever-more important instrument through which operators of social media and adjacent services – of their own volition – shape who can access their service and under what conditions. Indeed, many social media and gaming services use age as a determinant of which service features and functionalities are offered to individual users (e.g. Instagram Teen Accounts), and other services use age and age restrictions to curate their target user base (e.g. Tinder). In either case, whether to tailor the type of experiences or to curate the type of user base, companies are increasingly deploying, and children and adults encountering, various age assurance methods.

Beyond corporate policy considerations, for information society service providers subject to the EU digital *acquis,* age assurance has become an important means

through which they satisfy their regulatory due diligence obligations. Whether it is to ensure that the personal data of children is processed lawfully (pursuant to the General Data Protection Regulation), or to protect children from age-inappropriate exposure to pornography (pursuant to the Audiovisual Media Services Directive), service providers are increasingly relying on age assurance as a means of meeting their regulatory obligations in a proportionate manner.

Simply put, age assurance – in the manifold forms it takes – is becoming an ingrained feature both of experiencing, and of offering, online services in the EU today.

The Special Panel's recommendation adds to an ever-expanding global political and regulatory consensus on the proportionality of age assurance.

In recent years, numerous authoritative political and regulatory institutions in the EU and beyond have asserted the proportionality of fundamental rights-respecting age assurance for protecting children online.

In that regard, the Special Panel's report mirrors the requests of EU institutional stakeholders, including the European Parliament and the Council of the EU. It echoes the calls of multilateral bodies including the Council of Europe, the International Telecommunication Union, and the Organisation for Economic Co-operation and Development. And it aligns with the demands of European and third-country data protection authorities, who have elaborated what is required for age assurance to be proportionate and protective of privacy, data protection, and other fundamental rights [3].

This strong political consensus has engendered an uptick in multistakeholder efforts that engage with the complex balancing acts – of and among fundamental rights and system properties – that arise in age assurance deployments. Indeed, recent years have seen the emergence of substantive visions from various quarters for how to properly approach age assurance: at the policy level (e.g. how to design age assurance legislative mandates in accordance with the GDPR), at the deployment level (e.g. how to build age assurance systems that are meaningfully data minimising), and at the market level (e.g. how to ensure age assurance providers meet – and express adherence to – high standards for security and privacy).

As such, the global political and regulatory consensus around the need for age assurance, and the impetus it has given to efforts to conceive of rights-respecting policy frameworks and operational models, has created a favourable context within which the EU can develop an approach to age assurance that coheres with the Special Panel's vision.

[3] See for instance, European Parliament (2025); Danish Presidency (2025); Council of Europe (2018); OECD (2021); ITU (2020); EDPB (2025); ICO & Ofcom (2026).

A sector experiencing sustained waves of innovation and competition.

In response to regulatory requirements and market demand, the age assurance commercial sector has expanded rapidly in recent years. That expansion has coincided with a wave of technological innovation in age assurance products, with an ecosystem of vendors offering a variety of age assurance solutions[4]. Indeed, in 2026 the market for age assurance products ranges from facial and email-based age estimation, to credit card and mobile network operator checks, to digital identity-based solutions.

The rapid increase in age assurance deployments across the online sphere, the expansion in the vendor ecosystem, and the continued privacy, security, and inclusion concerns among adults and children, have been the catalyst for positive market developments. For instance, in an attempt to bring greater trust, accountability, and quality to the commercial ecosystem, standards development organisations and conformity assessment bodies have begun to establish criteria for how age assurance providers should operate and how their solutions should function. Likewise, a competitive and expanding market means providers in the ecosystem are increasingly incentivised to compete on privacy, usability, and interoperability, a reality that has contributed to, for instance, the proliferation of on-device data processing solutions and the emergence of mutual recognition schemes for age checks (Corby, 2026b)[5]. The development of the open-source EU Age Verification blueprint could help further support the sector's evolution in privacy and security.

Ultimately, as will be demonstrated later in this report, the dynamics of the age assurance market – where competition and innovation are prominent features – can be capitalised on by the legislator to mitigate both the fundamental rights interferences and cost burdens that a future legislative instrument would entail.

1.3. Structure of the report

Chapter 2 of the report will address the fundamental rights implications of age assurance, and advance recommendations on how negative interferences can be mitigated. The rights to data protection and privacy, non-discrimination, and freedom of expression and access to information will be treated in turn. Chapter 3 of the report will address the economic impact of a future legislative instrument

[4] See for instance: Biometric Update (2026) *Age Assurance & Digital Age Credentials Market Report*, Available at: https://www.biometricupdate.com/wp-content/uploads/2026/08/2026-age-assurance-digital-age-credentials-market-report.pdf

[5] Corby, I., (2026b) 'Rhetorically Conflating Age and Identity Checks Is Putting a Sign Above the Door You Want to Close'. Available at: https://avpassociation.com/thought-leadership/rhetorically-conflating-age-and-identity-checks-is-putting-a-sign-above-the-door-you-want-to-close/

on the information society service providers who are likely to be in scope. It will assess impacts and costs through both the deployment and the operational phases of compliance. Chapter 4 of the report will close with conclusions on how to realise a rights-respecting and proportionate age assurance ecosystem.

2. Fundamental rights impact

This report focuses on the three fundamental rights most directly engaged by the deployment of age assurance. These are the rights to data protection and privacy, the right to non-discrimination, and the right to freedom of expression and access to information. As noted in the introduction, it is beyond the scope of this report to treat fundamental rights questions that arise *prior* to the practical deployment of age assurance (e.g. whether age-based restrictions are compatible with the right to freedom of expression and access to information *per se*).

The attributes of a rights-respecting and effective age assurance system – such as accuracy, reliability, privacy, and inclusivity – cannot always be maximised simultaneously. Depending on how the legislator weighs these attributes against one another, a future legislative instrument might prescribe one or more specific methods and assurance levels for certain services or use cases. Alternatively, or for other services and use cases, it could set a general, outcomes-based mandate under which service providers can choose from a variety of methods to satisfy the age assurance regulatory requirement. The nature of the rights interferences, and the necessary mitigations, differ between these two regulatory scenarios, and the sections below distinguish between them where relevant[6].

2.1. Data protection and privacy

2.1.1. Mapping the rights interference

Age assurance, by definition, necessitates the processing of personal data – to assure the age or age range of an individual, the system must process *some* personal data pertaining to that individual. As such, the deployment of age assurance engenders an interference with individuals' right to privacy and the right to data protection as defined in the EU Charter of Fundamental Rights (EDPB, 2025)[7].

The degree of interference with these rights depends largely on the chosen method and deployment model for age assurance. Several methods – including facial age estimation and ID matching – require the processing of biometric data, and as such, might allow characteristics such as race or ethnicity to be inferred

[6] References in this chapter to a prescribed or specific method should be read as including cases where more than one method is prescribed. The key point is that service providers' choice in which age assurance methods to deploy is limited.

[7] European Data Protection Board (2025) *Statement 1/2025 on Age Assurance.* Available at: https://www.edpb.europa.eu/system/files/documents/2025-04/edpb_statement_20250211ageassurance_v1-2_en.pdf

(Sas & Mühlberg, 2024, p. 53)[8]. Other methods like behavioural inference models – while potentially not involving the processing of *special* categories of personal data – typically require the compilation and processing of significant *volumes* of personal data across numerous data sets (Shaffique & van der Hof, 2024)[9].

The risks associated with these interferences are not abstract or trivial. While the end-goal of age assurance might be to assure that an individual satisfies a minimum age baseline to access a service or to offer age-appropriate experiences, age assurance deployments could be utilised by service providers to collect far more data than that which is required to merely assure an individual's age or age range. The mere fact of this excessive collection – and especially when it occurs without transparency to the individual concerned – can be deeply intrusive and concerning for adults and children interacting with these systems[10].

Furthermore, data collected for the purpose of age assurance can be breached, leaking the personal data of individuals and exposing them to potential fraud, identity theft, blackmail, and other harms (Sas & Mühlberg, 2024)[11]. Where the age assurance method that is utilised by the service provider involves the processing of sensitive personal data (e.g. biometric data), the consequences for the rights and freedoms of individuals from such breaches can be even more profound and long-lasting[12].

Age assurance deployments can be used to facilitate the commercial profiling of individuals accessing a service. Absent guardrails on how services process personal data collected for the purpose of age assurance, there is a risk that the

---

[8] Sas, M., Mühlberg, J.T., (2024) *Trustworthy age assurance? A risk-based evaluation of available and upcoming age assurance technologies from a fundamental rights perspective,* p. 53, Available at: https://www.greens-efa.eu/files/assets/docs/age_assurance_v2.1.pdf

[9] Shaffique, M. R., van der Hof, S., (2024) 'Research report: Mapping age assurance typologies and requirements' , *European Commission DG CNECT,* Available at: https://digital-strategy.ec.europa.eu/en/library/research-report-mapping-age-assurance-typologies-and-requirements

[10] See, for instance, McConvey (2025b) 'Intermediary age assurance provider collecting user data on specific URLs, more'. Biometric Update. Available at: https://www.biometricupdate.com/202509/intermediary-age-assurance-provider-collecting-user-data-on-specific-urls-more

[11] Sas, M., Mühlberg, J.T., (2024) *Trustworthy age assurance? A risk-based evaluation of available and upcoming age assurance technologies from a fundamental rights perspective.* Available at: https://www.greens-efa.eu/files/assets/docs/age_assurance_v2.1.pdf

[12] In October 2025, the platform Discord disclosed that a third-party vendor handling age verification appeals was breached. Government ID photos and selfies (some showing users holding their ID alongside their Discord username) were potentially exposed, implicating roughly 70,000 users. See Silberling, A., (2025), Available at: https://techcrunch.com/2025/10/09/discord-suffers-data-breach-impacting-at-least-70000-users/

data collected can be used by service providers to enhance their profiling, micro-targeting, or identification of service users in pursuit of commercial objectives.

It is no surprise then that in recent years, data protection authorities (DPAs) across the EU have highlighted the risks to individuals' rights to privacy and data protection posed by age assurance deployments (EDPB, 2025; AEPD, 2023a; CNIL, 2021)[13]. And as regulatory explorations of age assurance for the purposes of protecting children have gathered pace, DPAs' privacy and security-focused concerns have been echoed and extended by digital rights advocates and scholars (CDT, 2026; Gruss *et al.*, 2026)[14].

Fortunately for the present policy reflection, many of these critical interventions have provided clear instruction on how interferences with privacy and data protection rights – and the harms to individuals that can subsequently arise – can be mitigated. To these mitigations we now turn.

2.1.2. How can it be mitigated?

The EU General Data Protection Regulation as a foundational safeguard.

While it is a horizontal regulatory framework applicable to a variety of forms of data collection and processing, the EU's General Data Protection Regulation (GDPR) speaks directly to the risks and harms associated with age assurance deployments. As articulated by the European Data Protection Board and national data protection authorities, all deployments of age assurance must be undertaken in a GDPR-compliant manner[15]. Strict adherence to, and enforcement of, the

---

[13] European Data Protection Board (2025) *Statement 1/2025 on Age Assurance.* Available at: https://www.edpb.europa.eu/system/files/documents/2025-04/edpb_statement_20250211ageassurance_v1-2_en.pdf

AEPD (2023a) 'Decalogue of principles Age verification and protection of minors from inappropriate content', Available at: https://www.aepd.es/guides/decalogue-principles-age-verification-minors-protection.pdf.

CNIL (2021) 'Recommendation 7: Check the age of the child and parental consent while respecting the child's privacy', Available at: https://www.cnil.fr/en/recommendation-7-check-age-child-and-parental-consent-while-respecting-childs-privacy

[14] Center for Democracy and Technology (2026) 'European Commission Announces Age Verification App, but Privacy, Security and Free Expression Concerns Remain', Available at: https://cdt.org/press/european-commission-announces-age-verification-app-but-privacy-security-and-free-expression-concerns-remain/

Gruss, D., et al. (2026), 'Joint statement of security and privacy scientists and researchers on age assurance', Available at: https://csa-scientist-open-letter.org/ageverif-Feb2026

[15] See EDPB (2025), AEPD (2023a), and CNIL (2022).

GDPR can address the substantive data protection and privacy concerns articulated above.

Of note with respect to age assurance:

- The GDPR's principle of **purpose limitation** can ensure that the data collected for the purpose of age assurance is not used by the service provider for another unrelated end. Strict and consistent enforcement of this provision could reduce the risk of age assurance mandates being leveraged by service providers for the purposes of user profiling.
- The GDPR's principle of **data minimisation** can ensure that age assurance systems collect the least amount of data necessary to assure an individual's age or age range. Excessive data collection is inherently harmful, it creates the risk of age assurance morphing into user identification, and it can heighten the adverse impact of data breaches on data subjects.
- The GDPR's **principle of transparency** can ensure that individuals can understand what personal data of theirs is collected, how it is processed and stored, who can access it, and when it is deleted. Strict application and enforcement of this principle can help overcome an often-cited concern among children and adults with respect to age assurance – that the systems and the practices of its deployers are opaque and untrustworthy.
- The GDPR's provisions on **data protection by design and default**, and its requirements that data controllers and processors implement appropriate **technical and organisational security measures**, should be robustly enforced in the age assurance domain, to ensure the risk to adults and children from data breaches and unlawful disclosure is minimised.

In essence, the GDPR offers a strong regulatory safeguard through which the interferences that age assurance poses to the rights to privacy and data protection can be managed and mitigated. While legal protections are only ever as effective as their enforcement by regulatory authorities and their adherence by service providers, the GDPR is nonetheless a key instrument that can be leveraged alongside a future EU-level legislative instrument to ensure the protection of children and the protection of all individuals' personal data go hand-in-hand.

The characteristics of age assurance deployment models.

Capitalising on technological innovation

Every age assurance method and deployment model involves some attributional trade-offs. For instance, structural features of the chosen method, and

operational choices made in its deployment, can mean an age assurance system is easy to use for some individuals but exclusionary for others[16]. In that context, how an age assurance system treats personal data – its collection, processing, and storage – is a key variable that age assurance providers and service providers need to contend with when implementing a system that will be used by children and adults. The choices they make can determine whether and to what extent the interferences that such systems pose for privacy and data protection rights are mitigated.

Recent years have seen increasing preoccupation among regulators, researchers, and practitioners with how to develop privacy-preserving mechanisms for age assurance. These efforts have aimed variously at: minimising the quantity of personal data that a system requires to assure age (McConvey, 2025a)[17]; hardening deployment models against the risk of data leakage (AEPD, 2023b)[18]; and, obviating the need to disclose personal data to a relying party to prove possession of an attribute (CNIL, 2022)[19]. The EU should leverage advancements in the field of privacy-protective age assurance in a future legislative instrument, to mitigate the privacy and data protection risks associated with this kind of regulatory mandate.

As one example, data protection authorities in the EU have called for age assurance deployments to capitalise on the emergence of methods that are double-blind in design (EDPB, 2025, para. 34)[20]. Under this system architecture, age is assured by one entity and that assurance is transmitted in token form to the relying website via an independent channel (NHIMG, 2026)[21]. Consequently,

---

[16] For instance, in many countries an individual must be over the age of 18 to possess a credit card. Checking whether one possesses a credit card is a low-friction means of assuring they meet a certain age threshold, but it can be exclusionary given that credit cards are often less widely possessed by those within disadvantaged socio-economic demographics.

[17] See for instance: McConvey, J., (2025a) 'BorderAge promises 100% anonymous age assurance with hand gesture modality', Available at: https://www.biometricupdate.com/202501/borderage-promises-100-anonymous-age-assurance-with-hand-gesture-modality

[18] AEPD (2023b) 'Technical note: Description of the proofs of concept of systems for age verification and protection of minors from inappropriate content'. Available at: https://www.aepd.es/guides/technical-note-proof-of-concept-age-verification-systems.pdf

[19] CNIL (2022) 'Online age verification: balancing privacy and the protection of minors', Available at: https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors

[20] European Data Protection Board (2025) *Statement 1/2025 on Age Assurance,* para. 34. Available at: https://www.edpb.europa.eu/system/files/documents/2025-04/edpb_statement_20250211ageassurance_v1-2_en.pdf

[21] Non-Human Identity Management Group (2026) 'Double blind age verification', Available at: https://nhimg.org/glossary/double-blind-age-verification/

the age-restricted website can learn that a user is of age to use a website (but not acquire any additional personal data pertaining to that user), and the entity performing the age check can acquire what data is necessary to assure the user's age (but not learn which age-restricted websites the user is accessing).

Research into, and deployment of, double-blind architectures has accelerated in recent years, owing to their promise to reduce the personal data processing required to perform age checks, and owing to their potential to mitigate some of the risks associated with data breaches. For instance, double-blind architectures are required under the implementation standards for France's 2024 SREN law[22], and CNIL – the national data protection authority – has gone as far as to develop a technological demo of an idealised version of such a method (CNIL, 2022)[23]. Private age assurance service providers have likewise sought to capitalise on the growing interest in double-blind methods, with a number of providers either developing or already offering market solutions that facilitate the use of this form of privacy-preserving age assurance (AVPA, 2025)[24].

The architectural-level privacy-preserving properties afforded by double-blind systems can be paired with zero-knowledge proofs (ZKPs). ZKPs are cryptographic protections that enable an individual to demonstrate the truth of an assertion or possession of an attribute, without needing to disclose any of the underlying data that makes that statement true or which proves their possession of the relevant attribute (Future of Privacy Forum, 2026)[25]. When deployed robustly, ZKP-based age assurance methods further reduce the quantity of data processing required to assure age, and the number of entities who can gain access to such data during the process[26]. However, it should be recognised that generating a zero-knowledge proof can be computationally intensive, and the burden typically falls on the user's own device rather than a centralised server.

---

[22] France, *Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique* [Law No 2024-449 of 21 May 2024 to secure and regulate the digital space] ('SREN Law'), JORF No 0119, 22 May 2024.

[23] CNIL (2022) 'Online age verification: balancing privacy and the protection of minors', Available at: https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors

[24] Age Verification Providers Association (2025) 'Interoperable age assurance', Available at: https://avpassociation.com/interoperable-age-assurance/

[25] Future of Privacy Forum (2026) 'Unpacking age assurance: Technologies and trade-offs', Available at: https://fpf.org/wp-content/uploads/2026/01/FPF-Age-Assurance-v2.0.pdf

[26] As with any system deployment, poor or partial implementations of zero-knowledge proof-based approaches to age assurance can still pose privacy and security risks. See, for instance, Hancock, A. and Collings, P. (2025) 'Zero Knowledge Proofs Alone Are Not a Digital ID Solution to Protecting User Privacy'. Electronic Frontier Foundation. Available at: https://www.eff.org/deeplinks/2025/07/zero-knowledge-proofs-alone-are-not-digital-id-solution-protecting-user-privacy

This can create usability frictions for individuals who possess older or lower-specification mobile devices.

The two key privacy-preserving innovations outlined above, namely double-blind architecture and zero-knowledge proof cryptography, are replicated in the EU Age Verification blueprint, with technical fallback foreseen for cases where ZKP is infeasible[27]. Incorporating the blueprint within a future legislative instrument – and ensuring its availability for individuals across the European Union – would therefore give effect to the recommendation of DPAs and others that age assurance mandates should capitalise on the state of the art in privacy-preserving technologies.

Enhancing protection at the enrolment stage

Double-blind architectures and zero-knowledge proofs can make age assurance more privacy-protective in one sense. However, they leave unresolved the significant data protection and privacy interferences that occur at the stage of the process when an individual seeks to prove they meet the required age threshold to an age assurance provider (e.g. at the initial enrolment stage of a digital ID-based system like the EU Age Verification blueprint or in facial age estimation systems).

The challenge for age assurance providers is that typically, the more accurate a system is in assuring an individual's age, the more privacy-invasive it is likely to be (FOSI, 2023, p. 6)[28]. For instance, digital identity-based systems and ID matching systems normally require individuals to disclose hard identifiers like passports, national ID cards, and driving licences. These systems normally require a further biometric disclosure, to ensure the identifier corresponds to the individual seeking to assure their age (a practice known as 'binding')[29]. Likewise, facial age estimation systems – while not requiring the disclosure of hard identifiers – depend on the individual disclosing biometric data pertaining to their facial features.

While these methods of age assurance necessarily invoke privacy and data protection interferences at the initial enrolment stage, age assurance providers

---

[27] European Commission (2026) 'EU Age Verification Blueprint — the dedicated technical portal', Available at: https://ageverification.dev/

[28] Family Online Safety Institute (2023) 'Coming to terms with age assurance', p. 6, Available at: https://global-uploads.webflow.com/5f4dd3623430990e705ccbba/64b0011a158eea37fb7796c4_FOSI%20White%20Paper%20Coming%20to%20Terms%20with%20Age%20Assurance%20FOR%20WEBSITE.pdf

[29] In some cases, age verification providers can secure access to trusted third-party databases (e.g. those held by public health providers) negating the need for the end user to disclose a hard identity artefact.

and service providers can take steps to mitigate the risks and harms that can flow from their deployment. Many of these mitigations can be made manifest in the product policy and product security properties of these systems. For instance, more age assurance providers are now offering on-device biometric assessments, meaning the sensitive data does not need to be transferred to the provider's servers and exposed to additional privacy and security risks during the age check or system enrolment process[30]. Moreover, in response to concerns about how data is processed, stored, and protected, some leading service providers have adopted product policies that aim to minimise the length of time that user data is stored by the age assurance provider following an age assessment[31]. And amid concern about potential data breaches, age assurance providers are increasingly using standards and industry certification schemes as a means of establishing better market practices in transparency and user-facing accountability across the vendor ecosystem[32].

The role of standards and auditing

Beyond transparency, this recent emergence of standards and certification schemes for the age assurance sector has helped set a procedural benchmark for how actors in the ecosystem collect, store, and safeguard personal data through the age assurance process. For instance, deployers of the EU Age Verification blueprint must adhere to strict technical implementation requirements intended to ensure robust privacy and security properties[33]. Process-focused standards like ISO/IEC 27566-1 and IEEE 2089.1 articulate the design and operational safeguards and practices that age assurance providers can take to make age assurance privacy-protective and secure[34]. And conformity

---

[30] See, for instance: Flores (2026), PrivateID (2025), and Burt (2023)

[31] For instance, according to Yoti's product policy, biometric facial scans are deleted as soon as age is checked https://www.yoti.com/blog/facial-age-estimation-faq-frequently-asked-questions/. According to Ondato's product policy, its FAE system never stores personal data https://ondato.com/age-verification/

[32] See for instance, IEEE SA (2026) 'Trends in online age verification for 2026', Available at: https://standards.ieee.org/beyond-standards/trends-in-online-age-verification-for-2026/. See also the Age Verification Providers Association membership code of conduct (AVPA, n.d). Available at: https://avpassociation.com/membership/avpa-code-of-conduct/

[33] European Commission (2026) 'EU Age Verification Blueprint — the dedicated technical portal', Available at: https://ageverification.dev/

[34] Institute of Electrical and Electronics Engineers (2024) *IEEE 2089.1-2024 IEEE Standard for Online Age Verification*. New York: IEEE. Available at: https://ieeexplore.ieee.org/document/10542699; International Organization for Standardization/International Electrotechnical Commission (2025) *ISO/IEC 27566-1:2025 Information security, cybersecurity and privacy protection – Age assurance systems – Part 1: Framework*. Geneva: ISO. Available at: https://www.iso.org/standard/88143.html

assessment bodies and independent testing bodies have begun to emerge as signifiers of trust in the ecosystem, helping increase confidence in age assurance provider claims about privacy and security[35].

The take-up of, and adherence to, these standards could add an additional mitigation to the privacy and data protection rights interferences that attend age assurance deployments. In that context, the EU should consider in a future legislative instrument how to ensure age assurance deployments are scrutinised and audited for adherence to privacy and security requirements, and it should encourage and potentially incentivise the continued growth of the independent auditing ecosystem.

2.1.3. Conclusion and summary of recommendations

This analysis has illustrated how the use of age assurance amounts to an interference with children's and adults' right to privacy and right to data protection. Depending on the chosen method, how it is deployed, and the policies and practices of the service providers involved, that interference can engender significant risks and harms to those whose age is assured. When considering and developing a legislative instrument that mandates age assurance, the EU legislator must fully appreciate these privacy and data protection implications.

Yet this analysis has also shown that there exist technologies, practices, and regulatory safeguards that can mitigate the attendant risks and harms. Taken together, these elements offer a path forward for a privacy- and data protection-respecting EU-level approach to age assurance.

In that context, when developing a future legislative instrument, the European Commission should:

1. **Ensure legislative coherence with the GDPR**, and ensure data protection authorities in the EU are properly resourced to apply the GDPR principles and protections to age assurance deployments and service providers.
2. Ensure deployment models that are permissible under a future legislative instrument meet **high standards of privacy and security**, in terms of their product policies, system architectures, and technical approaches.
3. Encourage – and possibly incentivise – the development of, adoption of, and adherence to **technical standards** that establish privacy and security baselines for the age assurance sector.

[35] See, for instance, the Age Check Certification Scheme (ACCS), a UK-established conformity assessment body that evaluates age assurance providers against the requirements of data protection law, online safety law, and international standards. https://accscheme.com/

2.2. Non-discrimination

2.2.1. Mapping the rights interference

A major concern stemming from the deployment of age assurance systems is their potential to unfairly discriminate against certain individuals and social groups, and the risk that these systems can compound existing societal disparities. Risks of discrimination in the age assurance domain come in several forms, and their nature and likelihood can vary depending on the method of age assurance chosen, and how it is deployed.

First, methods of age assurance that require the possession of hard identifiers at the enrolment stage – as is typically the case for digital identity-based solutions like the EU Age Verification blueprint – can lead to discriminatory outcomes in relation to individuals who do not possess qualifying hard identifiers (5Rights Foundation, 2026, p. 37; Ofcom, 2024, p. 102)[36]. Across EU Member States the possession of identifiers like passports can vary across demographics, and certain groups like children, the elderly, those in socio-economically disadvantaged groups, and those of immigrant or undocumented backgrounds are often less likely to possess the kind of hard identifiers that age assurance providers demand. Without appropriate fallbacks, premising age assurance on the disclosure of hard identifiers could therefore discriminate against adults and children who meet the relevant age threshold to access a service, but who lack the specific artefact to prove it to an age assurance provider.

Second, there are two sub-risks specific to digital identity-based methods which, if unaccounted for, might lead to exclusionary outcomes. Digital identity-based solutions typically require individuals to be in possession of a smartphone with near field communication (NFC) capability. This could be exclusionary for individuals from socio-economically disadvantaged groups who cannot afford such devices (Corby, 2026a)[37]. While smartphone penetration is high across the

[36] 5Rights Foundation (2026) 'Age Assurance as a spectrum: A risk-based approach from a European perspective', p. 37. Available at: https://5rightsfoundation.com/wp-content/uploads/2026/02/5rights_AgeAssurance_FINAL.pdf See also: Ofcom (2024) 'Volume 5: What should services do to mitigate the risks of online harms to children?' In: Protecting children from harms online consultation, p. 102. Available at: https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/284469-consultation-protecting-children-from-harms-online/associated-documents/vol5-what-should-services-do-to-mitigate-risks.pdf?v=336054

[37] Corby, I., (2026a) 'Is the EU age verification app ready for a social media minimum age?' Available at:

https://avpassociation.com/thought-leadership/is-the-eu-age-verification-app-ready-for-a-social-media-minimum-age/

EU, there will still be individuals and communities for whom device access is an issue. In addition, where successful navigation of the enrolment element depends on the end user possessing a high standard of digital literacy, the elderly and other vulnerable groups in society who are more likely to lack such skills could be discriminated against (Sas & Mühlberg, 2024, p. 39)[38].

Third, age assurance methods that use AI – notably, facial age estimation (FAE) and methods that depend on algorithmic binding of hard identifiers – pose a risk of algorithmic bias. These systems could engender discriminatory outcomes on grounds such as age, race, and ethnicity (5Rights Foundation, 2021, p. 30)[39]. Recent evaluations by the US National Institute of Standards and Technology (NIST) (2024)[40] and the United Kingdom's Department for Science, Innovation, and Technology (2026)[41] have reaffirmed the longstanding observation that FAE systems' accuracy can vary depending on demographic factors. Separate from algorithmic bias, FAE deployments typically must utilise age buffers aligned with the model's mean absolute error (MAE), to account for model accuracy limitations in and around age thresholds (ACCS, 2025, p. 75)[42]. All else held equal, the use of buffers could lead to exclusionary outcomes when certain individuals, who are of age to access a service but who are also within the age assurance deployment's buffer age, are wrongly locked out of services (Ofcom, 2024, p. 101)[43].

Ultimately, these three cases are illustrative of outcomes wherein individuals who possess protected characteristics, or who form part of an already vulnerable group, could be wrongly – and disproportionately – excluded from access to

---

[38] Sas, M., Mühlberg, J.T., (2024) *Trustworthy age assurance? A risk-based evaluation of available and upcoming age assurance technologies from a fundamental rights perspective.* Available at: https://www.greens-efa.eu/files/assets/docs/age_assurance_v2.1.pdf

[39] 5Rights Foundation (2021) 'But how do they know it is a child? Age assurance in the digital world' Available at: https://5rightsfoundation.com/wp-content/uploads/2024/09/But_How_Do_They_Know_It_is_a_Child-1.pdf

[40] NIST (2024) 'NIST Reports First Results From Age Estimation Software Evaluation', Available at: https://www.nist.gov/news-events/news/2024/05/nist-reports-first-results-age-estimation-software-evaluation

[41] Department for Science, Innovation, and Technology (2026) 'Age Assurance Data Access Study', Available at: https://www.gov.uk/government/publications/age-assurance-data-access-study/age-assurance-data-access-study#scale-and-nature-of-the-issue

[42] ACCS (2025) 'Age Assurance Technology Trial PART A Main Report', p. 75 Available at: https://www.infrastructure.gov.au/sites/default/files/documents/aatt_part_a_digital.pdf

[43] Ofcom (2024) 'Volume 5: What should services do to mitigate the risks of online harms to children?' In: Protecting children from harms online consultation, p. 101. Available at: https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/284469-consultation-protecting-children-from-harms-online/associated-documents/vol5-what-should-services-do-to-mitigate-risks.pdf?v=336054

online services which they are entitled to use, and potentially subjected to unlawful discrimination.

Fortunately, there are means – pertaining to both how age assurance methods are designed, and the broader socio-technical system within which adults and children interact with them – that can mitigate the risk of discriminatory outcomes.

2.2.2. How can it be mitigated?

Leverage age assurance methods and deployment models that are capable of high standards of inclusivity and fairness.

The European Commission's Guidelines on measures to ensure a high level of privacy, safety and security for minors online encourage service providers to consider, before implementing an age assurance approach, how it performs in terms of non-discrimination (European Commission, 2025, s. 6.1.4)[44]. Different age assurance methods and deployment models have differing inclusivity and fairness properties, and inclusivity sits alongside other critical deployment attributes, such as privacy, accuracy, and reliability.

Drawing on the two regulatory scenarios outlined at the start of this chapter, the legislator's balancing exercise among privacy, accuracy, reliability, and inclusivity might lead it to prescribe a *specific* method of age assurance for certain contexts. Such a choice narrows the range of methods available to end users, and in this scenario, inclusivity and non-discrimination must largely be achieved within the context of the deployment model *itself* (e.g. by ensuring the method is available to, and usable by, all). Alternatively, in the scenario where the service provider has flexibility over the method to deploy, the diversity of the age assurance landscape – in terms of methods and approaches – itself can provide the lever for inclusion.

This section will consider two methods – digital identity-based methods such as the blueprint, and FAE – that are likely to form the cornerstone methods of age assurance under a future legislative instrument, whether as prescribed methods or as the most commonly utilised methods under a flexible framework. Potential inclusion and fairness risks relating to these methods have already been identified, but as will be shown below, these can be mitigated in the legislative and deployment phases.

---

[44] European Commission (2025) *Communication from the Commission – Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28(4) of Regulation (EU) 2022/2065, OJ C, C/2025/5519, 10.10.2025*, s. 6.1.4 ELI: http://data.europa.eu/eli/C/2025/5519/oj.

Digital identity-based methods (including the EU Age Verification blueprint)

As noted earlier, digital identity-based methods of age assurance typically require the end user to present a qualifying hard identifier – normally a chip-based passport or a national ID card – to enrol in the system and secure a digital proof-of-age attestation. An obvious and already discussed risk from this method is that it might unfairly exclude individuals who lack qualifying hard identifiers or who lack the prerequisite technology to perform remote enrolment (i.e. a smartphone with an in-built NFC chip).

The legislator can take steps to mitigate the exclusionary risks of this method, by offering fallback mechanisms for those unable to enrol through the 'digital-first' approach. More specifically, the legislator should ensure that enrolment routes are available that do not require the user to possess either an NFC-enabled smartphone or a chip-based qualifying identifier. These fallback mechanisms should be as broadly scoped as feasible, to account for the varied reasons why an individual might not be able to enrol in a digital-identity based system through the 'default' pathway (Corby, 2026a)[45]. This could include accepting a wider range of documents at enrolment (e.g. non-chip identity cards, residence permits) or allowing a wider body of trusted sources that already hold verified age data to issue proof-of-age attestations[46].

Most EU Member States already offer the possibility of enrolling in their national digital identity schemes via an in-person visit to a local municipal office or registry service, where the process can be completed 'manually' and with a broader range of age artefacts. Capacity in terms of this fallback approach does, however, vary across the Member States, and on the basis of current capacity, some Member States might struggle to meet surge demand for manual enrolment (Corby, 2026a)[47]. If – as is likely – the EU Age Verification blueprint becomes a method of compliance under a future legislative instrument on age assurance, it is imperative that Member States extend and properly resource this kind of 'manual' enrolment fallback option so that it is available in a timely manner to end users

---

[45] Corby, I., (2026a) 'Is the EU age verification app ready for a social media minimum age?' Available at:

https://avpassociation.com/thought-leadership/is-the-eu-age-verification-app-ready-for-a-social-media-minimum-age/

[46] For instance, some individuals – for various reasons - might be reluctant to undergo a manual enrolment process that involves interaction with a public authority.

[47] Corby, I., (2026a) 'Is the EU age verification app ready for a social media minimum age?' Available at:

https://avpassociation.com/thought-leadership/is-the-eu-age-verification-app-ready-for-a-social-media-minimum-age/

who are unable to complete the 'digital-first' route to accessing blueprint-based solutions.

Facial age estimation (FAE)

As noted, facial age estimation methods risk exposing individuals and communities to algorithmic bias. They also vary in accuracy rates in and around age policy thresholds. Ensuring inclusion and fairness where this method is deployed largely starts with the age assurance sector – how it develops, deploys, and evaluates deployments. In recent years, the tracking and rectification of bias and excessive mean absolute error rates (a yardstick for effectiveness of the solution for the purposes of protecting children) has become an increasing focus of attention for FAE providers and for oversight bodies. While the evaluation of the age assurance sector's efforts largely rests on vendor self-reporting, there is emerging independent assessment that offers confidence in the sector's trajectory.

Most notably, since 2024 the US National Institute of Standards and Technology has administered the Face Analysis Technology Evaluation Age Estimation & Verification (FATE AEV) evaluation programme, an ongoing study into the effectiveness and inclusivity of FAE systems[48]. The FATE AEV programme publishes periodic reports on the state of the technology and specific deployments' performance in lab conditions. While the ongoing evaluation has made clear that disparities still exist across user demographics and that accuracy around policy thresholds remains an issue, deployments of the FAE method are on the whole showing steady improvement in age-related accuracy and inclusivity across demographics (Burt, 2026)[49].

Moreover, even while declining to mandate FAE for the purposes of assuring the age of 13-17 year-old users in its 2025 regulatory codes of practice, the United Kingdom's online safety regulator Ofcom has signalled cautious optimism about its trajectory, noting 'that there are increasingly effective means of [assuring the age of 13-17 year olds using methods including FAE]' and that it anticipates that 'improvements and new solutions [including with respect to FAE] will continue to develop at pace' (Ofcom, 2025a, p. 208)[50].

---

[48] NIST (2026) 'Face Analysis Technology Evaluation (FATE) age estimation & verification', Available at: https://pages.nist.gov/frvt/html/frvt_age_estimation.html

[49] Burt, C., (2026) 'NIST biometric age estimation update shows demographic, accuracy gains', Available at: https://www.biometricupdate.com/202605/nist-biometric-age-estimation-update-show-demographic-accuracy-gains

[50] Ofcom (2025a) 'Volume 4: What should services do to mitigate the risks of online harms to children?' In: Protecting children from harms online statement, p. 208. Available at: https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-

In Australia, the Age Assurance Technology Trial – an external study commissioned by the government in preparation for the implementation of the Social Media Minimum Age (SMMA) Act – provides a rich insight into the contemporary state of the FAE sector, including in terms of inclusivity and age threshold-related accuracy. In its testing of 13 age estimation systems deployed in an Australian context, it found deployers to be 'responsive to privacy and fairness challenges' (ACCS, 2025, p.82)[51] and that systems 'generally performed well across diverse user groups' (Ibid., p. 76)[52]. But underscoring the challenge that remains, the report's authors noted that some deployments exhibited reduced accuracy among certain user groups near the age policy threshold, and that underrepresentation of indigenous populations 'remains a challenge' (Ibid., p. 76)[53].

The studies and assessments referenced in this report are notable in that they are rare examples of rigorous *independent* evaluation. In that context, when developing a future legislative instrument that allows or requires the use of FAE for age assurance, the legislator should consider how to establish oversight mechanisms that confirm that these methods actually achieve effective and non-discriminatory outcomes. Secondary legislation that elaborates the non-discrimination principles of the Article 28 DSA Guidelines on the Protection of Minors ('the Article 28 Guidelines'), or the leveraging of standards like ISO/IEC 27566-1, could be promising means of sustaining progress in the sector and reducing reliance on vendor self-assertions.

When no specific method is required for compliance, ensure choice of methods and fallback options.

Where, on the balance of the considerations of privacy, accuracy, reliability, and inclusivity, the legislator decides against prescribing a specific method of age assurance, the legal framework should encourage or indeed ensure that service providers subject to age assurance requirements offer end users a choice of multiple (preferably several) age assurance methods and deployments through which to undergo the assurance process.

Moreover, service providers should endeavour to deploy age assurance systems that incorporate fallback options composed of distinct methods, so as to mitigate the consequences of false negatives (whereby a system incorrectly classifies a

---

weeks/statement-protecting-children-from-harms-online/main-document/volume-4-what-should-services-do-to-mitigate-the-risks-of-online-harms-to-children.pdf?v=403139

[51] ACCS (2025) 'Age Assurance Technology Trial PART A Main Report', p. 82, Available at: https://www.infrastructure.gov.au/sites/default/files/documents/aatt_part_a_digital.pdf

[52] Ibid., p. 76

[53] Ibid., p. 76

user as under the minimum age restriction). While method choice is important for several reasons, it is crucial in cases where FAE is utilised as the service provider's primary method of assurance. FAE deployment models invariably incorporate a buffer age (in light of their MAE rate) that can mean users close to the age policy threshold can be wrongly denied access (ACCS, 2025, p. 75)[54]. This accuracy shortcoming, allied with the risk of potential bias across different demographics, means FAE should not be relied upon by service providers as the *sole* method of assurance without escalation or fallback, if fairness and inclusivity are to be realised.

Finally, irrespective of whether a specific method is prescribed, service providers should offer easy-to-use and responsive complaints-handling mechanisms for situations where users are unable to assure their age using the methods on offer. Where age assurance is deployed today, there is wide divergence in how systems address assurance failure in the user journey. Sometimes, the only option available to users who fail an age check is to repeat the check (Ofcom, 2026, p. 19)[55]. This approach is unsatisfactory, both because it creates a risk of wrongful access (an underage user can keep trying until the system returns a false positive), and because it is unresponsive to the needs of of-age users who, for whatever reason, are unable to successfully navigate the system using the available methods. Service providers should therefore ensure their age assurance deployment includes the possibility of escalating the age-check process to a dedicated user-complaints/user support channel.

Make inclusivity and non-discrimination guiding principles during deployment processes.

The legislator and service providers must recognise that all age assurance methods – beyond those analysed in detail in this section – can engender interferences with the right to non-discrimination if inappropriately deployed. This is particularly true if service providers seek to optimise their age assurance for one specific attribute (e.g. accuracy, friction), without taking account of the likely trade-offs in other system attributes (e.g. inclusivity) (CNIL, 2022)[56]. Simply put,

---

[54] ACCS (2025) 'Age Assurance Technology Trial PART A Main Report', p. 75. Available at: https://www.infrastructure.gov.au/sites/default/files/documents/aatt_part_a_digital.pdf

[55] Ofcom (2026) 'Report on the use of age assurance', p. 19. Available at: https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/age-assurance-report-2026/report-on-the-use-of-age-assurance.pdf?v=423162

[56] For instance, competency-based age assurance methods require the user to successfully complete a series of challenges, for which it is assumed that individuals falling below the age restriction are not expected to pass at that age of intellectual competency. These systems can lead to discriminatory outcomes in relation to those individuals who do not meet the assumed competency level that the deployer associates with their age group, for example, owing to a neurodivergence, age-related cognitive decline, or a medical condition impacting cognitive function. See: CNIL (2022) 'Online age verification: balancing privacy

an age assurance deployment model that is frictionless for the majority of a service's user base could easily serve to lock out a small number of eligible users whose situation or condition makes that deployment model inaccessible.

In the case that a future legislative instrument provides flexibility to service providers to choose the method and deployment model of age assurance, service providers must be guided by the principles of the Article 28 Guidelines, and only offer methods that achieve the Guidelines' non-discrimination criterion. Where a specific method is prescribed, the corresponding responsibility rests with the legislator and Member States, who must ensure that the prescribed method – including its enrolment and fallback routes – meets that same criterion.

2.2.3. Conclusion and summary of recommendations

Ultimately, to date, in jurisdictions where services are deploying age assurance at scale in response to a regulatory requirement – most notably Australia and the UK – there is no clear evidence (beyond anecdotal examples) that of-age users have been excluded or wrongly denied access to online services as a direct result of age assurance mandates. But in any event, a legislative instrument that requires online services to deploy age assurance will certainly give rise to *risks* of discrimination and will pose challenges for inclusion and fairness. The nature, likelihood, and severity of these risks vary by method of age assurance, and how it is deployed in online spaces.

In designing the legislative instrument, the legislator can take steps to mitigate what are foreseeable and well-documented risks, in the scenarios where specific age assurance methods are required and where service providers are given more flexibility in the choice of method. Specifically, the European Commission should:

1. Ensure that EU Member States **provide and adequately resource effective fallback enrolment routes** – including manual enrolment at national and local level, acceptance of a broader range of identity documents, and proof-of-age attestations from other trusted sources – so that individuals who lack qualifying chip-based hard identifiers, or who do not have access to an NFC-capable smartphone, are not precluded from using EU Age Verification blueprint-based solutions.
2. Consider developing **secondary legislation that elaborates the non-discrimination principles of the Article 28 Guidelines, or consider leveraging standards like ISO/IEC 27566-1**, to bring greater transparency, direction, and accountability to how age assurance providers and deployment models ensure non-discrimination.
3. Where a specific assurance method and level is not prescribed, ensure **choice and optionality** in the age assurance process. Specifically:

and the protection of minors', Available at: https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors

encourage or require that service providers offer a plurality of distinct age assurance methods, with fallback where a preferred method fails.

4. Irrespective of the method deployed, ensure that online services make provision for escalation and **user support channels.**

2.3. Freedom of expression and access to information

2.3.1. Mapping the rights interference

The deployment of age assurance necessarily engenders several distinct types of interference with children's and adults' fundamental right to freedom of expression and access to information[57].

The most cited such interference in the literature concerning age assurance focuses on the restriction that it places on children's ability to engage with certain types of online spaces and certain forms of online content (Livingstone, *et al.,* 2024; EDRi, et al., 2024; Collings, 2026)[58]. However, this analysis will not engage with that specific interference. This analysis instead assesses fundamental rights interferences in the context where an age assurance mandate is *active*. This assumes the legislator has determined that restricting access to certain online spaces and content – despite its interference with children's right to freedom of expression – is necessary and proportionate, and that it strikes a fair balance against other relevant interests and objectives.

Taking inspiration from the age assurance two-part proportionality schema outlined in Shaffique & van der Hof (2024, p. 37)[59], this analysis will assess

---

[57] It also engenders an interference with service providers' freedom to impart information, as understood under the Charter. However, consideration of this interference is beyond the scope of this analysis.

[58] Livingstone, S. et al., (2024) 'Children's rights and online age assurance systems: The way forward' In: *The International Journal of Children's Rights*, Available at: https://brill.com/view/journals/chil/32/3/article-p721_009.xml; EDRi et al., (2024) 'Joint Statement on the Dangers of Age Verification Proposals to Fundamental Rights Online'. Available at:

https://edri.org/wp-content/uploads/2024/09/Joint-Statement-on-Dangers-of-Age-Verification.pdf; Collings, P., (2026) 'Internet Age Gates Are a Growing Global Threat', *Electronic Frontier Foundation.* Available at: https://www.eff.org/deeplinks/2026/06/internet-age-gates-are-growing-global-threat

[59] Shaffique, M. R., van der Hof, S., (2024) 'Research report: Mapping age assurance typologies and requirements', *European Commission DG CNECT,* p. 37. Available at: https://digital-strategy.ec.europa.eu/en/library/research-report-mapping-age-assurance-typologies-and-requirements

whether and to what extent the negative impacts of freedom of expression interferences that arise at the stage when age assurance is being *operationalised* can be mitigated through regulatory design, deployment choices, and safeguards.

For the purposes of this analysis then, two forms of freedom of expression and access to information interferences – one direct and experiential, and one diffuse and perceptual – warrant treatment.

Impact on adults and of-age child users.

A legislative instrument that sets a minimum age for social media access would invariably lead to a significant uptick in adults' direct exposure to age assurance. While the practice of assuring one's age has become an ever-more common feature of adults' everyday online experience *generally* (as discussed in chapter 1), many adults who hold social media accounts have never had to assure their age on those services specifically[60]. Moreover, they are likely to consider age assurance as being warranted for their online activities that have a comparable 'offline' age restriction (e.g. buying alcohol, viewing pornography, etc.) and not for online activities and spaces that are typically considered in their minds to be lower risk (Revealing Reality, 2022, p. 12)[61].

The introduction of an age assurance mandate for social media will invariably create unease for adults, as well as for of-age children who have already surpassed the minimum age. In a context where there is considerable concern about the privacy and data protection risks of age assurance, some of-age users might be unwilling to accept the obligation to assure their age as a pre-condition of access to social media, and they might instead opt out of service usage (Ofcom, 2024, p. 49)[62]. Although section 2.2.3 notes the lack of clear evidence yet of of-age users being wrongly *locked out* of accessing services in jurisdictions where age assurance mandates are in place, the fact of age assurance could still nudge individuals to alter their engagement with online services in a manner that

---

[60] This is predominantly because where they have opted to implement age assurance of their own volition in recent years, most social media services have prioritised low-friction age inference mechanisms in the first instance, meaning many adult accounts are never flagged as requiring dedicated age checks.

[61] Revealing Reality (2022) 'Families' attitudes towards age assurance', p. 12, Available at: https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/online-research/keeping-children-safe-online/families-attitudes-towards-age-assurance-/drcf-ofcom-ico-age-assurance.pdf?v=328566

[62] Ofcom (2024) 'Volume 5: What should services do to mitigate the risks of online harms to children?' In: Protecting children from harms online consultation, p. 49. Available at: https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/284469-consultation-protecting-children-from-harms-online/associated-documents/vol5-what-should-services-do-to-mitigate-risks.pdf?v=336054

has implications for freedom of expression. There is some relevant precedent for this phenomenon, with one study finding that 47% of surveyed individuals had reduced their consumption of pornography following the 2025 introduction of an age assurance requirement for adult services in the UK (Lucy Faithfull Foundation, 2026)[63]. While there are unique contextual factors involved in age assurance for access to pornography – the social taboo surrounding pornography means many users consider the data protection and privacy risks associated with age assurance to be particularly severe relative to other use cases – the UK experience points to an interference with freedom of expression and access to information that is a foreseeable consequence of mandating age assurance for social media access.

Furthermore, the requirement for adults to assure their age for social media access will invariably introduce more friction into their online experience. While this friction creates its own frustrations for adult users of social media, the greater concern arises from its proximity to an adjacent fundamental rights impact that was explored in the last section – namely, fairness and inclusion. In situations where adults and of-age children are unable to assure their age, owing to poor deployment models or because they lack the prerequisite identifiers or technology, the exclusionary outcome engenders a corresponding interference with their right to freedom of expression and access to information (Ofcom, 2024, p. 49)[64].

The broader perception and concern about long-term impacts and scope creep.

Public critiques of age assurance mandates often draw upon the longstanding suspicion that age assurance is the first step towards pervasive online identification and surveillance (Lorenz, 2026; Bhatia, 2026; Mullvad, 2026)[65].

---

[63] Lucy Faithfull Foundation (2026) 'Age verification has changed the way adults are watching porn', Available at: https://www.lucyfaithfull.org.uk/age-verification-has-changed-the-way-adults-are-watching-porn/

[64] Ofcom (2024) 'Volume 5: What should services do to mitigate the risks of online harms to children?' In: Protecting children from harms online consultation, p. 49. Available at: https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/284469-consultation-protecting-children-from-harms-online/associated-documents/vol5-what-should-services-do-to-mitigate-risks.pdf?v=336054

[65] Lorenz, T., (2026) 'The world wants to ban children from social media, but there will be grave consequences for us all' In: *The Guardian.* Available at: https://www.theguardian.com/commentisfree/2026/mar/02/ban-children-social-media-biometic-data-surveilled; Bhatia, A., (2026) 'Upload government papers to go online? That may be our new terrifying future', In: *The Guardian.* Available at: https://www.theguardian.com/commentisfree/2026/may/12/website-age-verification-government-identification; Mullvad (2026) 'Age verification for social media – the beginning

For the age assurance methods that are likely to form the cornerstone of a future EU age assurance framework – including digital identity-based solutions and facial age estimation – these concerns, whether substantiated or not, are directly relevant. For example, some stakeholders have argued that leveraging digital identity-based methods for the purposes of age assurance – as the EU Age Verification blueprint does – creates a technical infrastructure that could be leveraged for mass corporate and state surveillance (Gruss *et al.,* 2026)[66]. Moreover, some stakeholders have argued that the proliferation of FAE deployments – should it be encouraged by a future legislative instrument – would have the effect of normalising the routine disclosure of sensitive biometric data to third parties, and it would fundamentally alter future generations' understanding of the sensitivity of that data category (Sas & Mühlberg, 2024, p.33)[67].

Irrespective of the merits of these critiques, their prevalence within the public discourse surrounding age assurance could well mean that some adults and children are unwilling to engage with age assurance systems as the prerequisite for social media access. Moreover, where sceptical of-age users *do* opt to engage with the age assurance process, concern about surveillance and generalised identification might have a chilling effect on how they express themselves online and how they leverage social media to receive information. In both cases, the negative and unintended impacts on freedom of expression are obvious.

2.3.2. How can it be mitigated?

It should be noted that by implementing the recommendations outlined in the earlier sections of this chapter (those concerning data protection and non-discrimination), the legislator can likely make considerable progress towards mitigating the specific risks and harms identified in the section above. Nonetheless there are additional actions – building on the experiences of other jurisdictions where age assurance mandates are in place – that should be taken by the legislator in a future legislative instrument.

Minimise friction and optimise for user empowerment

As with the non-discrimination impacts noted above, the precise mitigations turn in part on the regulatory scenario within which age assurance is deployed (e.g.

of the end for a free internet?'. Available at: https://mullvad.net/en/blog/age-verification-for-social-media-the-beginning-of-the-end-for-a-free-internet

[66] Gruss, D., et al., (2026), 'Joint statement of security and privacy scientists and researchers on Age Assurance', Available at: https://csa-scientist-open-letter.org/ageverif-Feb2026

[67] Sas, M., Mühlberg, J.T., (2024) *Trustworthy age assurance? A risk-based evaluation of available and upcoming age assurance technologies from a fundamental rights perspective,* p. 33, Available at: https://www.greens-efa.eu/files/assets/docs/age_assurance_v2.1.pdf

whether services are mandated to use a specific method, or whether they have flexibility of methods).

First, where the legislator prescribes a specific method for certain services, choice will largely be operationalised within that method rather than across methods – for instance, through a choice of onboarding routes, attestation issuers, or blueprint-based apps and providers. Given that the perception of the age assurance provider *is itself* a factor in user preferences (as will be explored below), choice among providers can help address users' reluctance to engage with the age assurance process.

Where the legislator opts not to prescribe a *specific* method of age assurance for certain services or use cases, it can safeguard freedom of expression by requiring or encouraging service providers to offer a plurality of different age assurance methods or deployments for end users to choose between. This would respond directly to the situation where users opt out of assuring their age owing to concerns about a *specific* age assurance method or deployment (rather than the principle of age assurance itself) or because they lack the necessary technology/identity artefacts. When considering what methods to deploy, the legislator and service providers should take account of the reality that individuals' preferences with respect to age assurance are complex and heterogeneous, and turn on factors including friction, perception of the age assurance provider, perception of the method involved, and the nature of the activity for which age is being assured. Research into parents' and children's attitudes in the UK found that 'families rarely had a clear preference for one method over another as they also acknowledged that there were trade-offs to be made, for example between the effectiveness of a method and the effort required' (Revealing Reality, 2022, p. 6)[68]. Service providers should therefore avoid *assuming* the likely preferences of adults and children seeking to access their service.

Second and relatedly, where no specific method is prescribed, the legislator should permit and encourage companies to adopt 'successive validation' approaches in their age assurance deployment, to reduce friction and alleviate the burden that age assurance places on of-age users seeking to access their service. Successive validation – also known as 'waterfalling' – is a deployment strategy whereby users seeking to access a restricted service are subjected to the lightest-touch, lowest-friction age assurance method first, and the system falls back to higher-friction, more invasive methods only if the user fails to pass the

[68] Revealing Reality (2022) 'Families' attitudes towards age assurance', p. 6, Available at: https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/online-research/keeping-children-safe-online/families-attitudes-towards-age-assurance-/drcf-ofcom-ico-age-assurance.pdf?v=328566

prior age challenge (ICO, 2024)[69]. The Australian eSafety Commissioner – which is responsible for implementing the country's social media minimum age restriction – has endorsed successive validation as a means by which in-scope service providers can reduce friction for adult users and avoid disproportionate interferences with freedom of expression. In its guidance to industry, the regulator notes that 'requiring all existing Australian account holders to prove their age using an age verification system may be unreasonable and is not necessary for compliance – particularly in circumstances where the provider could use existing data to infer with reasonable confidence that certain end users are over 16' (eSafety Commissioner, 2025, p. 28)[70]. Likewise, Ofcom, the UK regulator responsible for implementing age assurance duties under the UK Online Safety Act (OSA), has implied its support for successive validation as a means of complying with the OSA's age assurance duties[71].

The low-friction quality of successive validation stems from the fact that methods utilised for the initial age check can often be satisfied without the end user being required to provide any additional personal data or take any proactive steps. As a case in point, in its recent roll-out of age assurance for iOS users in some jurisdictions, Apple opted for a deployment model that initially focuses on the age of the end user's Apple account, to assess whether it had been active for at least as long as the service's minimum age for users (if the account has been active for 18 years, it is reasonable to infer that the associated user is at least 18 years of age). The system also prioritises a check of whether there is a credit card associated with the user account (in the jurisdictions in question, one must be 18+ to possess a credit card). Only if these checks fail does the system fall back to the more invasive and higher-friction method of ID matching[72].

Successive validation deployment approaches significantly reduce the negative user-experience and inclusion impacts that age assurance processes have on of-

---

[69] Information Commissioner's Office (2024) 'Age assurance'. Available at: https://ico.org.uk/for-organisations/advice-and-services/audits/data-protection-audit-framework/toolkits/age-appropriate-design/age-assurance/

[70] eSafety Commissioner (2025) 'Social Media Minimum Age: Regulatory guidance' p. 28. Available at: https://www.esafety.gov.au/sites/default/files/2025-09/eSafety-SMMA-Regulatory-Guidance.pdf?v=1787047094674

[71] Ofcom's regulatory guidance concludes that age assurance methods typically associated with 'successive validation' strategies, including credit card checks, open banking approaches, and mobile network operator checks, are capable of meeting the regulatory standard for highly-effective age assurance. See Ofcom (2025c) 'Statement: Age assurance and children's access'. Available at: https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-age-assurance-and-childrens-access/statement-age-assurance-and-childrens-access.pdf?v=397036

[72] See the relevant Apple support page for further information: https://support.apple.com/en-gb/125662

age users, and they reduce the need for of-age users to undertake invasive age assurance processes that might engender a chilling effect on their freedom of expression. In an ideal outcome, in situations where providers have flexibility over the method deployed, it should mean that only a small number of of-age users are required to engage with digital identity-based, FAE, or equivalent methods.

It should of course be acknowledged that most successive validation techniques, such as credit card checks or email-based age estimation, are designed for assuring that an individual is over the age of 18, and as such, might not be suitable mechanisms for assuring the age of an individual who is above the minimum age threshold for access to social media but not yet an adult (e.g. ages 15-17). Moreover, the lower-friction methods that typically sit at the top of a successive validation waterfall rely largely on age inference and are generally less accurate and reliable than verification-based methods – a reality which would likely inform a legislator's rationale to restrict their use for certain age assurance use cases. In situations where the legislator prescribes certain age assurance methods or attributes, successive validation approaches that incorporate a broader range of lower friction, lower accuracy methods might not be feasible, although a narrower form – for example, first checking whether a user already holds a reusable proof-of-age attestation before prompting fresh enrolment – might remain possible. In any event, successive validation can be an extremely useful means of reducing the negative impacts of age assurance on of-age users under a future age assurance regulatory framework.

Third and finally, a source of frustration for of-age users that could lead them to turn away from social media use is 'assurance fatigue' – the situation where they are required to repeatedly assure their age to access a service and comparable ones. Although less of a concern for social media age assurance than other age assurance use cases – as service access is typically mediated by user accounts rather than unique session instances – the sheer number of services likely to be in scope of a legislative instrument and the likely requirement for services to ensure periodic assurance of account holders mean assurance fatigue is a foreseeable impact.

Fortunately, within the age assurance sector there are emerging proposals that could – among other benefits – help reduce assurance fatigue. These proposals aim to create the technical and operational means to ensure interoperability and mutual recognition of age checks across multiple age assurance providers. Projects including euCONSENT's AgeAware and k-ID's OpenAge are creating the infrastructure to enable interoperable, lower-friction age-checking[73]. Moreover, third-party age assurance providers are increasingly offering reusable age tokens, which allow a single age check to assure a user across multiple

[73] These solutions are discussed in detail in section 3.2.

websites[74]. This reusable token capability is likewise incorporated within the EU Age Verification blueprint offering[75]. Ultimately, in situations where service providers are required to use a specific method of age assurance (e.g. verification methods) for certain high-risk scenarios, reusability and interoperability, rather than method choice or successive validation, will likely be the key means through which friction and assurance fatigue are reduced.

Meaningful engagement and clear transparency.

The legislator must engage seriously with the public concern that age assurance mandates for social media might be the building blocks for a generalised online surveillance and identity capture regime. Irrespective of the veracity of, and justification for, these beliefs, their mere *propagation* can engender negative interferences with freedom of expression.

Engagement in this context should be transparency-focused, and it should occur at both the regulatory implementation stage and at the stage wherein individuals practically engage with age assurance systems.

In the first stage, legislators and regulators should take meaningful steps to communicate to the public the rationale for and proportionality of the age assurance mandate, and the steps that are being taken to address the precise concerns that have been illuminated in this report (e.g. the focus on privacy-preserving approaches; the offering of multiple assurance methods or onboarding routes; etc.). In public outreach, particular attention should be paid to communication with vulnerable groups and those with less experience of age assurance and comparable digital technologies. Simply put, adults and children should not be surprised when they encounter their first age check pursuant to a future legislative instrument. They should know what is happening, why, and how[76].

When age assurance systems *are* deployed – and when adults and children actively engage with them – the legislator should ensure deployers provide end

---

[74] See for instance: McConvey, J., (2025c) 'One check to rule them all: quest for reusable age assurance to ramp up in 2026', Available at: https://www.biometricupdate.com/202512/one-check-to-rule-them-all-quest-for-reusable-age-assurance-to-ramp-up-in-2026

[75] The blueprint supports reusable attestations where ZKP presentation is used, with each attestation valid for a maximum of three months. See European Commission (2026) 'EU Age Verification Blueprint – the dedicated technical portal'. S. 3.4.3. Available at: https://ageverification.dev/

[76] Although more broadly focused on minimum age restrictions, the Australian eSafety Commissioner's public-facing communications and engagement campaign in the lead up to the entry into force of the AU Social Media Minimum Age Act provides several relevant best practices on how the legislator can engage adults and children with age assurance regulatory change. See: https://www.esafety.gov.au/about-us/industry-regulation/social-media-age-restrictions-hub

users with clear, accessible, and age-tailored information about how systems operate, how data is handled and stored, and what supports are available in the case where an age-check is failed. While much of this transparency will in any event be required to make age assurance lawful under the GDPR (EDPB, 2025, para. 26)[77] , the legislator should ensure that all aspects of the age assurance interaction and user journey are designed with transparency and accountability to the end user in mind. This deployment ethos can help address user unease and anxiety about the fact of having to undertake age assurance for social media access.

Privacy-preserving deployment models allied with strong enforcement of the GDPR.

As with all the problematic interferences and impacts identified in this report thus far, concerns relating to freedom of expression and access to information can be significantly mitigated through a legislative focus on privacy-preserving age assurance deployment models and strong enforcement of the GDPR.

Many of the problematic freedom of expression interferences are born out of data protection and privacy concerns: individuals choose not to engage with age assurance systems, or alter their behaviour following an age check, because of concerns of identification and tracking. By ensuring the legislative instrument directs service providers towards the state of the art in privacy-preserving technologies and deployment models, these concerns can be mitigated. This is particularly important in cases where the legislator prescribes a specific method of age assurance: as users cannot opt for an alternative method, the privacy-preserving properties of the prescribed method itself – such as data minimisation and the unlinkability of age checks – become the principal safeguard against the chilling effects described in section 2.3.1.

Moreover, where concerns relate to how age assurance deployers collect and handle personal data, strict and effectively communicated enforcement of the GDPR by data protection authorities can mitigate some of the concerns that drive individuals to change their online behaviour in ways that are problematic from a freedom of expression perspective. Formal safeguards exist, but as already mentioned, they are only as effective as their enforcement and people's faith in them.

In essence, while freedom of expression considerations are distinct from those related to data protection and privacy, there is no pathway to trusted and accountable age assurance that does not flow through privacy-preserving deployments and enforcement of data protection law.

---

[77] European Data Protection Board (2025) *Statement 1/2025 on Age Assurance.* para. 26. Available at: https://www.edpb.europa.eu/system/files/documents/2025-04/edpb_statement_20250211ageassurance_v1-2_en.pdf

2.3.3. Conclusion and summary of recommendations

The problematic interferences with freedom of expression and access to information are closely related to, and in many cases direct results of, the other fundamental rights interferences that have been explored in this chapter.

Through a mix of dedicated interventions, alongside the implementation of recommendations outlined elsewhere in this report, the legislator can mitigate the problematic freedom of expression interferences that can follow from an age assurance deployment.

In particular, the legislator should:

1. **Minimise friction and optimise for user empowerment:** where no specific method is prescribed, by requiring or incentivising service providers to offer multiple age assurance methods or deployments and by permitting successive validation-style systems; where a specific method is prescribed, by ensuring choice of onboarding routes, attestation issuers and providers within that method; and in all cases, by encouraging greater interoperability and reusability of age checks across the age assurance market.
2. **Prioritise meaningful communication and clear transparency to individuals interacting with age assurance systems,** both at the regulatory implementation stage, and in the user experience of the practical age assurance process.
3. Build the regulatory framework around technologies and deployment models that are capable of being **privacy-preserving,** and ensure strict compliance with the **GDPR's** provisions.

3. Financial impact

3.1. Deployment costs

The EU Age Verification blueprint

It is likely that the EU Age Verification blueprint will be a cornerstone method of age assurance under a future legislative instrument. However, before assessing the blueprint's contribution to alleviating the economic burdens on service providers, it must be acknowledged that there is currently a lack of clarity as to whether and how Member States or third parties deploying solutions based on the EU Age Verification blueprint will seek to recover deployment, operational, and per-check costs. Moreover, age credential apps based on the blueprint are currently available in only a small number of EU Member States (European Commission, 2026)[78]. This deployment gap must be addressed as a matter of priority by Member States before any legislative instrument comes into effect.

That said, there is good reason to believe that the blueprint is likely to be, in time, among the cheapest means by which service providers can deploy age assurance in response to a future legislative instrument. The development cost of the blueprint has been publicly funded, and its technical architecture has been made available by the European Commission in open-source format for Member States and third-party deployers. While there will be some technical and administrative costs related to integrating the EU Age Verification blueprint-based solutions within service providers' operations, and while solution providers might seek to monetise age checks performed pursuant to it, arising costs are likely to be insignificant for reasons outlined in the sections below.

Besides the EU Age Verification blueprint, the financial cost of deploying an age assurance system for in-scope service providers largely turns on whether a service provider chooses to build a proprietary in-house age assurance system or chooses instead to procure a ready-made solution from a third-party age assurance vendor.

Proprietary in-house solutions

The deployment of a proprietary in-house age assurance system involves unique start-up costs that are likely to be significant. These include costs related to the initial code production as well as the testing required to ensure conformity with

[78] European Commission (2026) *EU Age Verification Blueprint — the dedicated technical portal*. Available at: https://ageverification.dev/

operational requirements (e.g. robustness, accuracy, etc.). Moreover, development of proprietary systems will likely necessitate the procurement of comprehensive training data and the provision of dedicated secure cloud storage infrastructure. These 'hard' development costs are likely to be supplemented by legal, compliance, and product policy costs.

As a case in point, in its 2025 impact assessment of its protection of children codes of practice, the UK regulator Ofcom estimated that hard costs relating to the development, deployment, and testing of an in-house age assurance system for the UK market 'could be in the region of many hundreds of thousands and potentially up to £1 million' and that total staff costs in this start-up phase (e.g. legal, compliance, etc.) 'may exceed this amount' (Ofcom, 2025b, p. 11)[79]. While the UK regulator has since sought to collect data on the costs that companies who have developed in-house solutions have incurred, it has found evidence to be 'limited and fragmented', with most service providers unable to isolate system development and deployment costs (Ofcom, 2026, p. 52)[80]. In any case, given the likely costs and complexity involved, it can be reasonably assumed then that the choice of deploying a proprietary in-house solution is one that is only likely to be exercised by the largest service providers, if at all.

Third-party solutions

Deployment costs are likely to be significantly lower for service providers who opt to leverage third-party age assurance solutions as a means of complying with a future legislative instrument. While existing data on the costs involved in deploying third-party solutions is limited, Ofcom's evaluation of the implementation of age assurance rules in the UK has found that 'set up costs do not appear high' (Ibid., p. 49)[81].

In Australia, the government impact assessment preceding the SMMA Act estimated that implementing an age assurance system that meets the requirements of the law would cost in-scope service providers approximately

---

[79] Ofcom (2025b) 'Volume 5: Annexes' In: *Protecting children from harms online: Statement*, p. 11. Available at: https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-protecting-children-from-harms-online/main-document/volume-5-annexes.pdf?v=396652

[80] Ofcom (2026) 'Report on the use of age assurance', p. 52. Available at: https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/age-assurance-report-2026/report-on-the-use-of-age-assurance.pdf?v=423162

[81] Ibid., p. 49. Available at: https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/age-assurance-report-2026/report-on-the-use-of-age-assurance.pdf?v=423162

EUR 4,200, expressed in 80 hours of staff time (DITRDCSA, 2024, p. 11)[82]. While not explicitly clarified, this calculation appears to assume that service providers would implement *third-party* solutions rather than build proprietary in-house systems (an approach which would invariably be far more intensive and costly)[83].

More broadly, as demand for age assurance solutions has increased across the tech ecosystem, implementation cost and friction are increasingly important factors on which third-party age assurance vendors compete. For instance, the third-party provider Yoti has asserted that service providers can integrate with its age assurance back-end within approximately half a day (DSIT, 2024, p. 61)[84]. iDenfy, another third-party provider, has asserted that its API-based solutions can typically be integrated by service providers 'within a week'[85]. And the identity provider Didit has asserted that its third-party age assurance solution can be made production-ready within days[86]. While these are vendor self-assertions and are not based on independent evaluations, they nonetheless point to a market dynamic wherein competing on speed and ease of integration is a priority.

For micro-enterprises and SMEs in particular, the emergence of 'plug-and-play' solutions and ready-made platform integrations can further reduce the cost of integrating age assurance within their operations. For instance, several third-party age assurance providers have developed plugins for the website builder platforms WordPress and Shopify among others, offering a relatively simple means by which service providers can complete the age assurance integration process. As a case in point, iDenfy asserts that its lighter weight plug-in-based solution can be deployed by service providers into their existing website platforms 'in minutes'[87], an assertion echoed by its competitor AgeVerif[88].

---

[82] Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts (2024) 'Impact Analysis Equivalent Supplementary Analysis OIA24-08210: Social Media Age Limit', p. 11. Available at: https://oia.pmc.gov.au/sites/default/files/posts/2024/11/Supplementary%20Analysis%20-%20Social%20Media%20Age%20Limit.pdf

[83] A note on methodology: all monetary figures in this chapter from USD, AUD, and GBP have been converted to EUR, at 27 August 2026 currency conversion rates.

[84] Department for Science, Innovation, and Technology (DSIT) (2024) 'Online Safety Act enactment impact assessment', p. 61. Available at: https://assets.publishing.service.gov.uk/media/6716222b9242eecc6c849b09/Online_Safety_act_enactment_impact_assessment.pdf

[85] See https://idenfy.com/integrations/

[86] See https://didit.me/solutions/age-verification/

[87] See https://idenfy.com/integrations/

[88] AgeVerif (2026) 'AgeVerif is now available in the Shopify App Store'. Available at: https://blog.ageverif.com/ageverif-is-now-available-in-the-shopify-app-store/

Ultimately then, given the lower costs and reduced friction involved, most small and medium-sized services will opt to procure third-party solutions for age assurance rather than develop and deploy their own. Moreover, while much of today's data is based on vendor self-assertions, from the available evidence and market commentary it is reasonable to assume that the costs of integrating third-party solutions for most small- and medium-sized services will be in the hundreds of euro or the low thousands of euro (assuming one to several software developer days at standard market rates).

3.2. Ongoing costs

Analysis of the ongoing costs of complying with a future legislative instrument on age assurance should be bifurcated into operational costs and per-check costs.

Operational costs

Every service will be obliged to devote resources to sustain the operation of its age assurance system. These costs are varied, and include legal costs, compliance costs, information security costs, customer support costs, and supplier due diligence costs. These costs invariably scale with the volume of age checks undertaken, and are likely to be costs more easily absorbed by large service providers who already have significant mid- and back-office operational infrastructure.

Operational costs are likely to be lower for services that rely on third-party age assurance solutions compared with those that operate proprietary in-house systems. This is because in third-party system deployments, much of the ongoing system maintenance, operational security, and due diligence is handled by the age assurance vendor directly.

The Australian government, in its impact assessment for the SMMA Act, predicted that in-scope providers would likely be required to devote 10 hours of staff time per week to 'business-as-usual' compliance in the first year of the law coming into force (equating to approximately EUR 27,300 annually). It further predicted that this requirement would drop to two hours of staff time per week in subsequent years (equating to approximately EUR 5,450 annually) (DITRDCSA, 2024, p. 11)[89]. In the UK, service providers have thus far been unable to accurately quantify the operational costs associated with their age assurance deployments. Nonetheless, Ofcom has asserted that 'while [operational type]

[89] Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts (2024) 'Impact Analysis Equivalent Supplementary Analysis OIA24-08210: Social Media Age Limit', p. 11. Available at: https://oia.pmc.gov.au/sites/default/files/posts/2024/11/Supplementary%20Analysis%20-%20Social%20Media%20Age%20Limit.pdf

costs may represent an additional cost for businesses and be relevant in some cases, the evidence we reviewed does not allow us to conclude they prevented the effective deployment of age assurance for the analysed service providers' (Ofcom, 2026, p. 50)[90].

Per-check costs

The per-check costs of age assurance will again likely vary across the industry. Per-check costs are easier to isolate and analyse in situations where the service provider relies upon a third-party age assurance provider, as the per-check cost is often the key variable on which vendors charge and compete.

In its report on the implementation of UK age assurance requirements, Ofcom estimated that the per-check cost incurred by the evaluated service providers had a median of around EUR 0.07, with most checks falling at or below a cost of EUR 0.12 (Ibid., p. 51)[91]. Prior to the entry into force of the UK's age assurance requirement, the regulator had predicted that per-check costs would range between EUR 0.06 and EUR 0.35 (Ofcom, 2025b, p. 9)[92], while the UK government had estimated the average per-check cost to be EUR 0.14 (DSIT, 2024, p. 60)[93]. The Australian government, in its impact assessment for the SMMA Act, has predicted per-check costs to be approximately EUR 0.39 per check (DITRDCSA, 2024, p. 11)[94].

A number of factors influence the ultimate price that service providers pay on a per-check basis. Different pricing models exist across the industry, including

---

[90] Ofcom (2026) 'Report on the use of age assurance', p. 50. Available at: https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/age-assurance-report-2026/report-on-the-use-of-age-assurance.pdf?v=423162

[91] Ibid., p. 51

[92] Ofcom (2025b) 'Volume 5: Annexes' In: *Protecting children from harms online: Statement*, p. 9. Available at: https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-protecting-children-from-harms-online/main-document/volume-5-annexes.pdf?v=396652

[93] Department for Science, Innovation, and Technology (DSIT) (2024) 'Online Safety Act enactment impact assessment', p. 60. Available at: https://assets.publishing.service.gov.uk/media/6716222b9242eecc6c849b09/Online_Safety_act_enactment_impact_assessment.pdf. Note that the impact assessment monetary value is expressed in 2021 prices, and has been adjusted here for inflation to 2026 prices.

[94] Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts (2024) 'Impact Analysis Equivalent Supplementary Analysis OIA24-08210: Social Media Age Limit', p. 11. Available at: https://oia.pmc.gov.au/sites/default/files/posts/2024/11/Supplementary%20Analysis%20-%20Social%20Media%20Age%20Limit.pdf

subscription models, fixed-cap models, and volume-tiered models. Many vendors appear to offer tailored packages depending on contextual factors and the volume of likely checks to be completed (Ofcom, 2026, p. 51)[95].

Analysis of market pricing practices and the implementation of age assurance requirements in the UK suggests that per-check marginal costs are typically inversely related to the volume of checks undertaken (Ibid., p. 51)[96]. Put differently, the more checks completed, the cheaper each check becomes for the service provider. This reality is likely to be a benefit for larger service providers, who, owing to the size of their user base, will presumably undertake the most age checks by volume under a future legislative instrument. Indeed, industry observers have noted that for some large companies with high volumes of checks, the average per-check price of age assurance under existing UK and Australian rules has been below EUR 0.06 (Allen, T., 2026, pers. comm.)[97].

Market analysis suggests that the per-check cost of age assurance is informed in part by the chosen method (Ofcom, 2026, p. 82)[98]. In that context, service providers' per-check costs can be alleviated by implementing a 'successive validation' approach to the assurance process, in instances where the regulatory framework provides flexibility for choice of compliance method. As seen in section 2.3.2, successive validation is a deployment strategy whereby users seeking to access a restricted service are subjected to the lightest touch, lowest-friction age assurance method first, and the system falls back to higher-friction, more invasive methods only if the user fails to pass the prior age challenge. In that vein, a future legislative instrument that provides service providers with flexibility to choose an age assurance method for compliance should encourage services to utilise approaches that are low cost and low-friction (e.g. age of the user's account) in the first instance, while reserving higher-cost checks only for user accounts where the user's age cannot be initially assured with confidence. Where a specific method and assurance level is prescribed, the reusability of proof-of-age attestations – a feature of digital identity-based solutions, including the EU Age Verification blueprint, discussed below – can be an important means of reducing per-check costs over time.

---

[95] Ofcom (2026) 'Report on the use of age assurance', p. 51. Available at: https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/age-assurance-report-2026/report-on-the-use-of-age-assurance.pdf?v=423162

[96] Ibid., p. 51. Available at: https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/age-assurance-report-2026/report-on-the-use-of-age-assurance.pdf?v=423162

[97] Allen, T., 2026, personal communication.

[98] Ofcom (2026) 'Report on the use of age assurance', p. 82. Available at: https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/age-assurance-report-2026/report-on-the-use-of-age-assurance.pdf?v=423162

As a method, the digital identity-based nature of the EU Age Verification blueprint suggests it would amount to a cost-competitive per-check solution for service providers subject to a future legislative instrument. Recent experience in the UK offers an insight into the potential cost reduction benefits involved. While take-up of digital ID-based age assurance solutions has been low under the UK's Online Safety Act, the limited evaluation data from Ofcom suggests that digital ID-based solutions are among the cheapest available to service providers on a per-check basis. Indeed, most evaluated services that are deploying digital ID-based solutions in the UK reported per-check costs of EUR 0.00 (Ofcom, 2026, p. 82)[99]. This finding likely stems from the reality that digital ID-based solutions typically incorporate reusable proof-of-age attestations and do not incur per-check costs, with third-party age assurance providers instead monetising through other, paid verification services bundled alongside the free digital ID check. A different mechanism produces a similar outcome for the EU Age Verification blueprint: rather than commercial cross-subsidy, the underlying infrastructure has been publicly funded and made available in open-source format, meaning the initial technical development costs need not be recovered on a per-check basis from relying parties. As such, it is reasonable to assume that service providers are likely to face low or minimal ongoing per-check costs under a future legislative instrument, in the case that they rely on the EU Age Verification blueprint as an age assurance method.

Broader considerations

It should be noted that most large services (and some medium-sized ones) will likely have some form of existing age assurance architecture in place, whether owing to corporate trust & safety considerations or emanating from a pre-existing regulatory mandate in the EU or a third country. The fact of having a pre-existing age assurance architecture in place (whether proprietary or of the third-party kind) is likely to alleviate some of the additional costs for these service providers under a future legislative instrument. For these service providers, compliance with an EU-level age assurance mandate could be achieved through the extension and expansion of an age assurance architecture, and they will likely be able to capitalise on some of the previous investments made in developing or integrating those systems. Evidence of this phenomenon can be seen in the UK, where some service providers have reported not incurring *any* set-up costs associated with the jurisdiction's age assurance mandate (Ibid., p. 49)[100]. The regulator attributes this finding to the reality that many service providers have existing commercial

[99] Ofcom (2026) 'Report on the use of age assurance', p. 82. Available at: https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/age-assurance-report-2026/report-on-the-use-of-age-assurance.pdf?v=423162

[100] Ofcom (2026) 'Report on the use of age assurance', p. 49. Available at: https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/age-assurance-report-2026/report-on-the-use-of-age-assurance.pdf?v=423162

relationships and operational integrations with third-party age assurance vendors, meaning the provision of additional age assurance services to meet a compliance requirement can be executed without meaningful additional implementation resource.

Separately, a factor that is likely to reduce per-check costs for service providers in the medium term is the advancement of interoperability of age assurance deployments. As already discussed, projects including euCONSENT's AgeAware and k-ID's OpenAge are creating the infrastructure to enable an age check completed by one age assurance provider to be recognised by another age assurance provider with whom an online service has a commercial relationship[101]. This advancement could enable the cost of age checks and the cost of provisioning a multi-method age assurance deployment to be shared across participating service providers. Illustrative of the potential of interoperability models to reduce costs, k-ID has asserted that reusing an age credential issued by a participating service provider costs other participating service providers 'just fractions of a cent' per use[102]. That said, the early stage of development and deployment of these interoperability solutions means it is not yet possible to accurately predict the medium-term cost reduction benefits to service providers that might accrue from them.

3.3. Longer term economic projection

Robust data on the cost impacts of age assurance is admittedly limited. Allied with this, the global age assurance sector is experiencing waves of expansion and innovation, meaning assessments based on today's market realities are likely to be soon superseded. Nonetheless, certain reasoned macro-level predictions about the likely medium term economic impact of a future legislative instrument can be inferred, based on the trends in the age assurance market.

First, per-check costs of third-party age assurance solutions are likely to continue to decrease, as technology advances and the global market for age assurance solutions grows more competitive. This prediction is largely based on comparable experiences in other software-as-a-service-based competitive markets during periods of market growth and expansion. In its impact assessment for the Online Safety Act, the UK government's Department for Science, Innovation, and Technology noted that 'types of age assurance solutions, their accuracy, and their availability are rapidly evolving. The government and industry expect technology

[101] See: AgeAware: https://euconsent.eu/interoperability-through-ageaware-from-euconsent/; OpenAge: https://k-id.com/news-posts/openage-initiative-launched

[102] See: https://openageinitiative.org/

to greatly improve in this market' (DSIT, 2024, p. 59)[103]. Moreover, in its impact assessment of how it would implement those rules, the regulator Ofcom asserted its belief that 'there is a significant likelihood that costs of age assurance will fall over time' (Ofcom, 2025b, p. 11)[104].

Second, the advancements in interoperability are likely to place further downward pressure on per-check costs of age assurance. While still nascent, the marketisation of interoperability will almost certainly accelerate in the coming years, particularly as more small and medium-sized enterprises implement age assurance systems. Besides reducing user friction, the key benefit of interoperability is its potential to reduce per-check costs for participating service providers.

Third, advancements in standardisation will enhance the quality and trust of third-party vendors in the market. While the rapid expansion in the age assurance vendor ecosystem has resulted in increased choice and competition, service providers procuring third-party age assurance solutions must today place faith in the credentials of vendors and devote resources towards vendor due diligence and ongoing quality control. While this is to be expected in a still-young sector experiencing rapid expansion, it nonetheless creates risk, complexity, and cost for service providers. In that context, the emergence of standards – including ISO/IEC 27566-1:2025 and IEEE 2089.1-2024 – is a positive development. These standards, which set baselines for how age assurance deployments should operate and how they should achieve outcomes like accuracy and privacy, should serve to elevate practice and quality across the sector, thereby easing the due diligence burden on service providers who will need to procure age assurance solutions in the coming years.

Fourth, in a context wherein age assurance is becoming an increasingly global norm, there are significant compliance economies of scale for companies operating across borders. Many services (particularly large ones) have already developed proprietary or procured third-party age assurance solutions in response to regulatory requirements in other contexts. As age assurance becomes an increasingly relevant operational consideration, service providers active across borders will be able to amortise the fixed costs of deployment, technical integration, and internal compliance processes across a far larger operational base, rather than developing jurisdiction-specific compliance

---

[103] Department for Science, Innovation, and Technology (DSIT) (2024) 'Online Safety Act enactment impact assessment', p. 59. Available at: https://assets.publishing.service.gov.uk/media/6716222b9242eecc6c849b09/Online_Safety_act_enactment_impact_assessment.pdf.

[104] Ofcom (2025b) 'Volume 5: Annexes' In: *Protecting children from harms online: Statement*, p.11. Available at: https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-protecting-children-from-harms-online/main-document/volume-5-annexes.pdf?v=396652

solutions in isolation. Relatedly, the harmonising effects of a dedicated EU-level age assurance instrument would further reduce operational and compliance costs for service providers, who would no longer need to tailor their general age assurance approach to the regulatory idiosyncrasies of various EU Member States.

Fifth, regulation will likely serve as a stimulus for further innovation in technology and market offerings. The introduction of binding age assurance duties in the UK and Australia has coincided with expansion in the number and sophistication of age assurance vendors operating in those markets (Corby, I., 2026, pers. comm.)[105]. This is consistent with the broader pattern – observed in adjacent regulatory domains – whereby the creation of legal certainty and clear compliance demand accelerates investment and new entrant activity. A future EU-level instrument could reasonably be expected to generate a comparable stimulus effect, particularly given the scale of the EU Single Market as a demand signal for third-party age assurance providers. As noted by the trade body the Age Verification Providers Association, 'clear legal requirements also stimulate supply […] regulatory certainty can resolve this chicken-and-egg problem and expand choice after day one' (AVPA, 2026a, p. 34)[106].

3.4. Impact on SMEs

Depending on the scope of a future legislative instrument, it could well be the case that many micro-, small-, and medium-sized enterprises will be required to deploy or procure age assurance solutions for the first time. The likely impact of this is worthy of dedicated treatment.

The availability of the EU Age Verification blueprint has the potential to insulate micro-enterprises and SMEs from the most significant costs associated with an age assurance requirement. In line with the general trend of the third-party age assurance sector, the blueprint aims for ease of integration, meaning micro-enterprises and SME service providers should not need to devote disproportionate resource to incorporating a compliant age assurance solution within their business operations. Indeed, it is foreseeable that integration of blueprint-based EU age verification solutions for micro-enterprises and SMEs could cost within the range of hundreds of euro or low thousands of euro (one to several developer days at current market rates). It is admittedly more difficult to assess the likely *ongoing* costs of the EU Age Verification blueprint for micro-enterprises and SMEs. Legal, compliance, and user support costs will likely

[105] Corby, I., 2026, personal communication.

[106] AVPA (2026a) 'Age assurance at 16: Technology readiness for an under-16 social media account restriction', p. 34. Available at: https://avpassociation.com/consultation-response/age-assurance-at-16-white-paper/

depend on *how* these service providers choose to integrate the blueprint (e.g. via a government-developed solution or via a third-party trusted provider). The cost range of age checks themselves – although still unclear – will likely mirror the low rates associated with existing digital ID-based deployments.

Beyond the EU Age Verification blueprint, micro-enterprises and SMEs will benefit from the reality that third-party age assurance providers are increasingly competing on ease of integration. As noted above, third-party providers offer plug-and-play widgets, APIs, or specific plugins for website builder platforms like WordPress and Shopify. These approaches significantly reduce the upfront technical investment required of micro-enterprises and SMEs. Sector figures expect the volume and kind of age assurance services that directly target the needs of micro-enterprises and SMEs to increase should regulation create new market demand among these types of service providers (Corby, I., 2026, pers. comm.)[107].

Micro-enterprises and SMEs will likely face proportionally higher *per*-check costs than their larger competitors when using third-party solutions that do not rely on reusable proof-of-age credentials. Larger platforms are typically better positioned to negotiate volume-based discounts given the scale of their user base, whereas SMEs, processing far fewer verifications, are less able to access preferential per-unit pricing. However, the EU Age Verification blueprint offers a pathway for SMEs seeking to avoid this size disadvantage (as per-check marginal prices under digital identity-based solutions are typically very low). Moreover, the disproportionately higher per-check costs that micro-enterprises and SMEs face will likely be somewhat offset by the low initial deployment costs these services face, assuming they rely on the easy-integration solutions described above.

Micro-enterprises and SMEs are also likely to experience elevated operational and compliance costs relative to their size (e.g. user support in cases where the age challenge fails), as unlike larger services, they are less likely to have existing mid- and back-office infrastructure which can absorb these costs. However, as noted above, the operational cost burden on micro-enterprises and SMEs can be significantly reduced by their use of third-party privacy-preserving methods as well as solutions based on the EU Age Verification blueprint. The EU Age Verification blueprint and comparable methods reduce service providers' exposure to data protection and security risks, which are among the main operational and compliance cost drivers. Moreover, many third-party age assurance vendors manage user support and related operational issues as part of their service offering to clients.

As a final consideration, SMEs will likely benefit significantly from harmonised EU-level rules on age assurance, relative to larger services. As more and more EU Member States consider legislative proposals that require online services to

[107] Corby, I., 2026, personal communication.

deploy age assurance, regulatory fragmentation brings increased costs for smaller companies with limited compliance capacity. Under today's policy trajectory, online services will increasingly be required to procure and deploy bespoke solutions across the Union and devote more resources to compliance and administration, to adapt to differing regulatory requirements for age thresholds, acceptable buffer limits, allowable methods, and privacy and security standards. Because SMEs have more limited resources than larger services operating in the EU market, which can spread such costs across substantial revenue bases, this 'cost of non-Europe' in age assurance is more pronounced for them. And conversely, the benefits of regulatory harmonisation – while accruing to service providers of all sizes – would likely be more pronounced for smaller services.

3.5. Conclusion and summary of recommendations

This analysis has shown that a future age assurance mandate would place novel cost burdens on information society service providers, spanning deployment, ongoing operational, and per-check costs. The scale of that burden will vary and evolve, depending on the choice of deployment model, the evolution of the vendor market, and the size of the service provider concerned.

Yet this analysis has also shown that these costs are unlikely to be significant for many service providers, and steps can be taken by the legislator to alleviate them in the short and medium term. The EU Age Verification blueprint, the competitive dynamics of the third-party vendor market, the emergence of technical standards, and the harmonising effects of an EU-level instrument can each exert downward pressure on deployment and compliance costs.

In that context, when developing a future legislative instrument, the European Commission should:

1. **Accelerate the roll-out of the EU Age Verification blueprint across all Member States.** As the analysis in sections 3.1, 3.2, and 3.4 has shown, the blueprint's publicly funded, open-source architecture gives it the potential to be among the cheapest available compliance pathways for service providers of every size, including on a per-check basis. However, most EU Member States do not currently offer blueprint-based age assurance solutions that can be utilised by online services and end users within their jurisdiction. This deployment gap must be closed by Member States before any legislative instrument comes into effect.
2. **Permit and encourage deployment approaches that reduce friction and per-check costs.** Where no specific method is prescribed, this includes permitting successive validation, so that service providers can rely on low-cost, low-friction methods in the first instance and escalate only where necessary. In all cases, the legislator should support reusable

proof-of-age attestations and the continued development of interoperability and mutual recognition initiatives, which allow the cost of an age check to be spread across multiple relying service providers rather than borne separately by each.

3. **Develop secondary legislation and/or leverage the growth of technical standards to reduce vendor due diligence costs for service providers**. As discussed in section 3.3, standards such as ISO/IEC 27566-1 and IEEE 2089.1 have the potential to reduce the burden service providers currently face in vetting and monitoring third-party vendors, by establishing a trusted baseline that reduces reliance on vendor self-assertion. The legislator should consider how adherence to such standards can be encouraged or incentivised within any future instrument, or indeed complemented by dedicated EU secondary legislation. This would serve to enhance market quality and to reduce service providers' due diligence costs.

4. Conclusion

Age assurance, in whichever method or deployment model it takes, engenders interferences with fundamental rights. It interferes with the rights to data protection and privacy, and to freedom of expression. It carries foreseeable risks of discrimination and exclusion.

Age assurance places cost burdens on information society service providers, large and small alike. To deploy, operate, and maintain age assurance systems in accordance with any future legislative instrument, online service providers will be confronted with novel costs.

A future legislative instrument must appreciate these realities if it is to be proportionate and rights-respecting.

This report has shown that the rights interferences and economic costs associated with age assurance can be substantially mitigated through deliberate legislative design and policy implementation. Strict enforcement of the GDPR, the leveraging of privacy-preserving deployment architectures, and the provision of 'fallback' mechanisms are just some of the steps the legislator can take to make a future legislative instrument rights-respecting.

Likewise, by permitting successive validation techniques where no specific method is prescribed, by supporting reusable and interoperable age checks, and by leveraging advancements in the competitive dynamics of the third-party age assurance sector, the legislator can ensure the novel costs that service providers face are manageable.

The EU's Age Verification blueprint can make an important contribution to alleviating the interferences and impacts identified in this report, alongside comparable age assurance methods that prioritise privacy and ease of deployment. But the blueprint will only be as effective as its deployment, and prior to any legislative instrument coming into force, Member States must ensure blueprint-based solutions and supporting infrastructure are available to all service providers and individuals in the Union.

Ultimately, this report has demonstrated how the goal set by the co-chairs of the Special Panel on child safety online in their final report – that the European Commission advance an age assurance framework that is fundamental rights-respecting and proportionate – can be achieved.

Bibliography

AEPD (2023a) 'Decalogue of principles: Age verification and protection of minors from inappropriate content'. Available at: https://www.aepd.es/guides/decalogue-principles-age-verification-minors-protection.pdf

AEPD (2023b) 'Technical note: Description of the proofs of concept of systems for age verification and protection of minors from inappropriate content'. Available at: https://www.aepd.es/guides/technical-note-proof-of-concept-age-verification-systems.pdf

Age Check Certification Scheme (ACCS) (2025) *Age Assurance Technology Trial: Part A: Main Report*. Available at: https://www.infrastructure.gov.au/sites/default/files/documents/aatt_part_a_digital.pdf

Age Verification Providers Association (AVPA) (2025) 'Interoperable age assurance'. Available at: https://avpassociation.com/interoperable-age-assurance/

Age Verification Providers Association (AVPA) (2026a) 'Age assurance at 16: Technology readiness for an under-16 social media account restriction'. Available at: https://avpassociation.com/consultation-response/age-assurance-at-16-white-paper/

Age Verification Providers Association (AVPA) (n.d.) 'AVPA Code of Conduct'. Available at: https://avpassociation.com/membership/avpa-code-of-conduct/

AgeVerif (2026) 'AgeVerif is now available in the Shopify App Store'. Available at: https://blog.ageverif.com/ageverif-is-now-available-in-the-shopify-app-store/

Apple (2026) User support webpage detailing age assurance approach for iOS accounts. Available at: https://support.apple.com/en-gb/125662

Bhatia, A. (2026) 'Upload government papers to go online? That may be our new terrifying future'. *The Guardian*. Available at: https://www.theguardian.com/commentisfree/2026/may/12/website-age-verification-government-identification

Biometric Update (2026) *Age Assurance & Digital Age Credentials Market Report.* Available at: https://www.biometricupdate.com/wp-content/uploads/2026/08/2026-age-assurance-digital-age-credentials-market-report.pdf

Burt, C. (2023) 'Privately bringing on-device biometrics and age estimation to diverse market sectors'. *Biometric Update*. Available at:

https://www.biometricupdate.com/202301/privately-bringing-on-device-biometrics-and-age-estimation-to-diverse-market-sectors

Burt, C. (2026) 'NIST biometric age estimation update shows demographic, accuracy gains'. *Biometric Update.* Available at: https://www.biometricupdate.com/202605/nist-biometric-age-estimation-update-show-demographic-accuracy-gains

Center for Democracy and Technology (CDT) (2026) 'European Commission Announces Age Verification App, but Privacy, Security and Free Expression Concerns Remain'. Available at: https://cdt.org/press/european-commission-announces-age-verification-app-but-privacy-security-and-free-expression-concerns-remain/

CNIL (2021) 'Recommendation 7: Check the age of the child and parental consent while respecting the child's privacy'. Available at: https://www.cnil.fr/en/recommendation-7-check-age-child-and-parental-consent-while-respecting-childs-privacy

CNIL (2022) 'Online age verification: balancing privacy and the protection of minors'. Available at: https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors

Collings, P. (2026) 'Internet Age Gates Are a Growing Global Threat'. *Electronic Frontier Foundation*. Available at: https://www.eff.org/deeplinks/2026/06/internet-age-gates-are-growing-global-threat

Corby, I. (2026a) 'Is the EU age verification app ready for a social media minimum age?'. *Age Verification Providers Association (AVPA).* Available at: https://avpassociation.com/thought-leadership/is-the-eu-age-verification-app-ready-for-a-social-media-minimum-age/

Corby, I. (2026b) 'Rhetorically Conflating Age and Identity Checks Is Putting a Sign Above the Door You Want to Close'. *Age Verification Providers Association (AVPA*). Available at: https://avpassociation.com/thought-leadership/rhetorically-conflating-age-and-identity-checks-is-putting-a-sign-above-the-door-you-want-to-close/

Council of Europe (2018) *Recommendation CM/Rec(2018)7 of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment*. Strasbourg: Council of Europe. Available at: https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a

Danish Presidency of the Council of the European Union (2025) *The Jutland Declaration: Shaping a Safe Online World for Minors*. 10 October. Available at: https://www.digmin.dk/Media/638956829775203140/DIGMIN_The%20Jutland%

20Declaration%20Shaping%20a%20Safe%20Online%20World%20for%20Minors%20101025.pdf

Department for Science, Innovation, and Technology (DSIT) (2024) *Online Safety Act enactment impact assessment*. Available at: https://assets.publishing.service.gov.uk/media/6716222b9242eecc6c849b09/Online_Safety_act_enactment_impact_assessment.pdf

Department for Science, Innovation, and Technology (DSIT) (2026) *Age Assurance Data Access Study.* Available at: https://www.gov.uk/government/publications/age-assurance-data-access-study/age-assurance-data-access-study

Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts (DITRDCSA) (2024) *Impact Analysis Equivalent Supplementary Analysis OIA24-08210: Social Media Age Limit*. Available at: https://oia.pmc.gov.au/sites/default/files/posts/2024/11/Supplementary%20Analysis%20-%20Social%20Media%20Age%20Limit.pdf

Didit (n.d.) 'Age Verification'. Available at: https://didit.me/solutions/age-verification/

EDRi et al. (2024) 'Joint Statement on the Dangers of Age Verification Proposals to Fundamental Rights Online'. Available at: https://edri.org/wp-content/uploads/2024/09/Joint-Statement-on-Dangers-of-Age-Verification.pdf

eSafety Commissioner (2025) 'Social Media Minimum Age: Regulatory guidance'. Available at: https://www.esafety.gov.au/sites/default/files/2025-09/eSafety-SMMA-Regulatory-Guidance.pdf

eSafety Commissioner (2026) 'Social media age restrictions hub'. Available at: https://www.esafety.gov.au/about-us/industry-regulation/social-media-age-restrictions-hub

euCONSENT (2025) 'Interoperability through AgeAware from euCONSENT'. Available at: https://euconsent.eu/interoperability-through-ageaware-from-euconsent/

European Commission (2025) *Communication from the Commission – Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28(4) of Regulation (EU) 2022/2065, OJ C, C/2025/5519, 10 October 2025*. Available at: http://data.europa.eu/eli/C/2025/5519/oj

European Commission (2026) 'EU Age Verification Blueprint – the dedicated technical portal'. Available at: https://ageverification.dev/

European Data Protection Board (EDPB) (2025) *Statement 1/2025 on Age Assurance*. Available at: https://www.edpb.europa.eu/system/files/documents/2025-04/edpb_statement_20250211ageassurance_v1-2_en.pdf

European Parliament (2025) *Resolution of 26 November 2025 on the protection of minors online (2025/2060(INI)). P10_TA(2025)0299*. Strasbourg: European Parliament. Available at: https://www.europarl.europa.eu/doceo/document/TA-10-2025-0299_EN.html

Family Online Safety Institute (FOSI) (2023) *Coming to terms with age assurance.* Available at: https://global-uploads.webflow.com/5f4dd3623430990e705ccbba/64b0011a158eea37fb7796c4_FOSI%20White%20Paper%20Coming%20to%20Terms%20with%20Age%20Assurance%20FOR%20WEBSITE.pdf

Fegert, J. and Melchior, M. (2026) *Child Safety Online: Protecting and Empowering Minors in a Digital World*. Available at: https://commission.europa.eu/document/download/d833504d-5ec3-4fac-945f-38e7d0bd5326_en?filename=Special-panel-report.pdf

5Rights Foundation (2021) *But how do they know it is a child? Age assurance in the digital world*. Available at: https://5rightsfoundation.com/wp-content/uploads/2024/09/But_How_Do_They_Know_It_is_a_Child-1.pdf

5Rights Foundation (2026) *Age Assurance as a spectrum: A risk-based approach from a European perspective*. Available at: https://5rightsfoundation.com/wp-content/uploads/2026/02/5rights_AgeAssurance_FINAL.pdf

Flores, M. (2026) 'Introducing Incode On-Device Age Estimation, the First On-Device Age Assurance Solution With Enterprise-Class Privacy, Accuracy, and Security'. Incode. Available at: https://www.incode.com/blog/introducing-incode-on-device-age-estimation/

France (2024) *Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique ['SREN Law'],* JORF No 0119, 22 May 2024.

Future of Privacy Forum (2026) 'Unpacking age assurance: Technologies and trade-offs'. Available at: https://fpf.org/wp-content/uploads/2026/01/FPF-Age-Assurance-v2.0.pdf

Gruss, D. et al. (2026) 'Joint statement of security and privacy scientists and researchers on Age Assurance'. Available at: https://csa-scientist-open-letter.org/ageverif-Feb2026

Hancock, A. and Collings, P. (2025) 'Zero Knowledge Proofs Alone Are Not a Digital ID Solution to Protecting User Privacy'. *Electronic Frontier Foundation*.

Available at: https://www.eff.org/deeplinks/2025/07/zero-knowledge-proofs-alone-are-not-digital-id-solution-protecting-user-privacy

iDenfy (n.d.) 'Integrations'. Available at: https://idenfy.com/integrations/

IEEE SA (2026) 'Trends in online age verification for 2026'. Available at: https://standards.ieee.org/beyond-standards/trends-in-online-age-verification-for-2026/

Information Commissioner's Office (ICO) (2024) 'Age assurance'. Available at: https://ico.org.uk/for-organisations/advice-and-services/audits/data-protection-audit-framework/toolkits/age-appropriate-design/age-assurance/

Information Commissioner's Office (ICO) and Ofcom (2026) *Age assurance: a joint statement by Ofcom and the Information Commissioner's Office*. Available at: https://ico.org.uk/media2/5ybpmabf/ofcom-ico-joint-statement.pdf

Institute of Electrical and Electronics Engineers (2024) IEEE 2089.1-2024: IEEE Standard for Online Age Verification. New York: IEEE. Available at: https://ieeexplore.ieee.org/document/10542699

International Organization for Standardization/International Electrotechnical Commission (2025) ISO/IEC 27566-1:2025 Information Security, Cybersecurity and Privacy Protection — Age Assurance Systems — Part 1: Framework. Geneva: ISO. Available at: https://www.iso.org/standard/88143.html

International Telecommunication Union (ITU) (2020) *Guidelines for industry on Child Online Protection*. Geneva: ITU. Available at: https://www.unicef.org/media/90796/file/ITU-COP-guidelines%20for%20industry-2020.pdf

K-ID (2025) 'OpenAge initiative launched'. Available at: https://k-id.com/news-posts/openage-initiative-launched

Livingstone, S. et al. (2024) 'Children's rights and online age assurance systems: The way forward'. *The International Journal of Children's Rights*, 32(3), 721–747. Available at: https://brill.com/view/journals/chil/32/3/article-p721_009.xml

Lorenz, T. (2026) 'The world wants to ban children from social media, but there will be grave consequences for us all'. *The Guardian*. Available at: https://www.theguardian.com/commentisfree/2026/mar/02/ban-children-social-media-biometic-data-surveilled

Lucy Faithfull Foundation (2026) 'Age verification has changed the way adults are watching porn'. Available at: https://www.lucyfaithfull.org.uk/age-verification-has-changed-the-way-adults-are-watching-porn/

McConvey, J. (2025a) 'BorderAge promises 100% anonymous age assurance with hand gesture modality'. *Biometric Update*. Available at: https://www.biometricupdate.com/202501/borderage-promises-100-anonymous-age-assurance-with-hand-gesture-modality

McConvey, J. (2025b) 'Intermediary age assurance provider collecting user data on specific URLs, more'. *Biometric Update*. Available at: https://www.biometricupdate.com/202509/intermediary-age-assurance-provider-collecting-user-data-on-specific-urls-more

McConvey, J. (2025c) 'One check to rule them all: quest for reusable age assurance to ramp up in 2026'. *Biometric Update*. Available at: https://www.biometricupdate.com/202512/one-check-to-rule-them-all-quest-for-reusable-age-assurance-to-ramp-up-in-2026

Mullvad (2026) 'Age verification for social media — the beginning of the end for a free internet?'. Available at: https://mullvad.net/en/blog/age-verification-for-social-media-the-beginning-of-the-end-for-a-free-internet

National Institute of Standards and Technology (NIST) (2024) 'NIST Reports First Results From Age Estimation Software Evaluation'. Available at: https://www.nist.gov/news-events/news/2024/05/nist-reports-first-results-age-estimation-software-evaluation

National Institute of Standards and Technology (NIST) (2026) 'Face Analysis Technology Evaluation (FATE): Age Estimation & Verification'. Available at: https://pages.nist.gov/frvt/html/frvt_age_estimation.html

Non-Human Identity Management Group (NHIMG) (2026) 'Double blind age verification'. Available at: https://nhimg.org/glossary/double-blind-age-verification/

OECD (2021) *Recommendation of the Council on Children in the Digital Environment*. OECD/LEGAL/0389. Paris: OECD. Available at: https://legalinstruments.oecd.org/public/doc/272/272.en.pdf

Ofcom (2024) 'Volume 5: What should services do to mitigate the risks of online harms to children?' In: *Protecting Children from Harms Online (Consultation).* Available at: https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/284469-consultation-protecting-children-from-harms-online/associated-documents/vol5-what-should-services-do-to-mitigate-risks.pdf

Ofcom (2025a) 'Volume 4: What should services do to mitigate the risks of online harms to children?' In: *Protecting Children from Harms Online (Statement).* Available at: https://www.ofcom.org.uk/siteassets/resources/documents/consultations/catego

ry-1-10-weeks/statement-protecting-children-from-harms-online/main-document/volume-4-what-should-services-do-to-mitigate-the-risks-of-online-harms-to-children.pdf

Ofcom (2025b) 'Volume 5: Annexes'. In: *Protecting Children from Harms Online (Statement).* Available at: https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-protecting-children-from-harms-online/main-document/volume-5-annexes.pdf

Ofcom (2025c) *Statement: Age assurance and children's access.* Available at: https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-age-assurance-and-childrens-access/statement-age-assurance-and-childrens-access.pdf

Ofcom (2026) *Report on the use of age assurance.* Available at: https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/age-assurance-report-2026/report-on-the-use-of-age-assurance.pdf

Ondato (n.d.) 'Age verification'. Available at: https://ondato.com/age-verification/

PrivateID (2025) 'Age verification'. Available at: https://privateid.com/age-verification/

Revealing Reality (2022) *Families' attitudes towards age assurance.* Available at: https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/online-research/keeping-children-safe-online/families-attitudes-towards-age-assurance-/drcf-ofcom-ico-age-assurance.pdf

Sas, M. and Mühlberg, J.T. (2024) *Trustworthy Age Assurance? A Risk-Based Evaluation of Available and Upcoming Age Assurance Technologies from a Fundamental Rights Perspective*. Available at: https://www.greens-efa.eu/files/assets/docs/age_assurance_v2.1.pdf

Shaffique, M.R. and van der Hof, S. (2024) 'Research report: Mapping age assurance typologies and requirements'. *European Commission DG CNECT*. Available at: https://digital-strategy.ec.europa.eu/en/library/research-report-mapping-age-assurance-typologies-and-requirements

Shaffique, M.R. and van der Hof, S. (2026) 'Behavioural profiling for age assurance: do the ends justify the means?'. In: *International Data Privacy Law*, 16(1), ipaf012. Available at: https://academic.oup.com/idpl/article/16/1/ipaf012/8327959

Silberling, A. (2025) 'Discord data breach affects at least 70,000 users'. *TechCrunch*. Available at: https://techcrunch.com/2025/10/09/discord-suffers-data-breach-impacting-at-least-70000-users/

Yoti (2022) 'Facial age estimation FAQ'. Available at: https://www.yoti.com/blog/facial-age-estimation-faq-frequently-asked-questions/

Getting in touch with the EU

In person

All over the European Union there are hundreds of Europe Direct centres. You can find the address of the centre nearest you online (european-union.europa.eu/contact-eu/meet-us_en).

On the phone or in writing

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
- at the following standard number: +32 22999696,
- via the following form: european-union.europa.eu/contact-eu/write-us_en.

Finding information about the EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website (european-union.europa.eu).

EU publications

You can view or order EU publications at op.europa.eu/en/publications. Multiple copies of free publications can be obtained by contacting Europe Direct or your local documentation centre (european-union.europa.eu/contact-eu/meet-us_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex (eur-lex.europa.eu).

EU open data

The portal data.europa.eu provides access to open datasets from the EU institutions, bodies and agencies. These can be downloaded and reused for free, for both commercial and non-commercial purposes. The portal also provides access to a wealth of datasets from European countries.

KK-01-26-173-EN-N



Publications Office
of the European Union