Deloitte.

CENTRE *for*
REGULATORY
STRATEGY
EMEA

Online Age Assurance

Responding to the evolving European regulatory landscape

September 2025

The structure of this report

Click on the boxes to navigate to each section

EXECUTIVE SUMMARY

SECTION 1:
Key themes and criteria emerging from age assurance regulation in select European jurisdictions

This section explores key themes and criteria emerging from a cross-jurisdictional analysis of age assurance regulations, brought to life by two hypothetical case studies.

CASE STUDY 1:
Fictional social media company

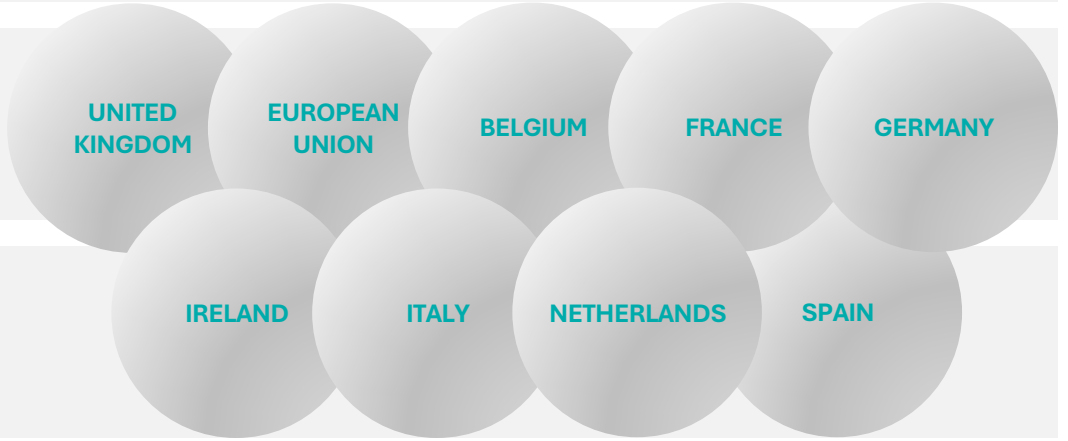
CASE STUDY 2:
Fictional online forum

SECTION 2:
Operational and strategic implications

This section outlines the operational actions and strategic implications for online services and how these can be addressed across the organisation.

SECTION 3:
Navigating age assurance requirements under specific European jurisdictions

This section maps age assurance regulations and initiatives across select European jurisdictions.



SECTION 4:
Terminology and Deloitte contacts

This section explains the terms used in the report and lists relevant Deloitte contacts across Europe.

Executive Summary

Online age assurance: responding to the evolving European regulatory landscape

- **Online age assurance is now a top regulatory priority,** arising from growing concerns about children's safety online. However, **the regulatory landscape is evolving and fragmented**, with a wide range of relevant regulations and differing national requirements.
- **Getting age assurance right is critical.** Failure to do so may expose firms to substantial financial penalties (up to 6% of global turnover in the EU and 10% of qualifying worldwide revenue in the UK), reputational damage, and erosion of user trust.
- This report first identifies **key regulatory themes**, as well as the **criteria guiding implementation** of age assurance regulation across select European countries. This comparative analysis does not evaluate the merits of age assurance requirements nor the effectiveness of different jurisdictions' regulatory approaches.
- It then outlines the **operational** and **strategic implications** for online services in Europe, to protect children from inappropriate online content.
- Lastly, it provides a snapshot of age assurance regulations in the UK, the EU and seven EU Member States.

- From an **operational perspective,** firms should:
  - Develop a **centralised compliance tracker** and **an effective early warning** system.
  - **Implement age assurance systems** that **(i)** are proportionate to service risks, **(ii)** balance safety with privacy-by-design, **(iii)** maximise accuracy, reliability and robustness, and **(iv)** ensure a non-discriminatory and accessible process.
  - Determine whether to **develop age assurance systems in-house or integrate a third-party solution**, and **when in the customer journey** to implement age checks.

- From a **strategic perspective,** firms should consider:
  - Their **geographic footprint** in light of different national requirements.
  - Their **product and service design** based on findings from risk assessments, particularly given expected increased scrutiny over service design more generally. Adopting an **age-appropriate design** may require substantive changes, such as tiered service models.
  - Whether, and if so how, to align their age assurance strategy with the **EU's age verification app** and planned **Digital Identity Wallets** to future-proof compliance.

Who is this report for?

- This report is relevant to providers of online user-to-user services, such as social media platforms, messaging apps, online marketplaces and online gaming. It is also relevant to those providers of audiovisual services (e.g. video sharing platforms) within the scope of audiovisual media services regulation. It does not cover age assurance requirements in sector-specific regulation directly focused on restricted services and products, such as gambling and the online sale of alcohol or tobacco.
- It should be of particular interest to the senior management and heads of trust and safety responsible for shaping a company's online safety strategy, as well as risk, compliance and regulatory affairs leads.

Section 1

Key themes and implementation criteria relevant to online age assurance in select European jurisdictions

01

Introduction

The internet is central to children's lives, relevant to how they access entertainment, education, social connection and more. In this context, online age assurance has rapidly ascended the policy agenda in the UK and EU, driven by concerns over children's exposure to harmful content and behaviours. In response, policymakers and regulators are demanding stronger safeguards.

This is an area that is also central to public debate. Proponents assert that age assurance is essential to protecting children online, whilst some critics argue that it risks negatively impacting other areas such as privacy and free speech. Early moves by in-scope companies to introduce age checks have been widely reported in the media, as have attempts to circumvent these checks (for example using Virtual Private Networks). Such considerations are outside the scope of this report, which instead focuses on how in-scope companies can respond to relevant regulatory requirements.

At EU level, the protection of minors and age assurance is a priority for the European Commission, with finalised **guidelines on the protection of minors online** published on 14 July 2025. At the same time, a number of EU Member States are arguing for mandatory age verification for access to social media.

It is also notable that the European Commission is developing an age verification app which is expected to set the standard for online age assurance in the EU and bridge the gap before the roll-out of **EU Digital Identity (EUDI) Wallets**, expected for next year.

Nonetheless, there remains **significant fragmentation and evolving requirements** across national jurisdictions, including within the EU. At the national level, some countries are mandating age verification for multiple service types while others are lacking binding requirements even for services that pose a high risk to minors, like pornography.
This ultimately raises **complexity for in-scope services:**

- Within a single jurisdiction, **multiple regulations need to be considered**, in particular **online safety regulation**, **data protection regulation** and, for some online services, **audiovisual media services regulation**.
- There are **a range of possible approaches to age assurance and acceptable methods vary across jurisdictions**. For example, facial age estimation is considered to be an overly intrusive and non-compliant method by AGCOM in Italy in relation to services disseminating pornographic content, whilst it is considered capable of being highly effective by Ofcom in the UK.
- Services may need to **balance both compliance and wider business interests.** For example, imposing overly onerous or high-friction age assurance systems may impact user acquisition and retention.

Ultimately, getting age assurance right is necessary for maintaining user trust whilst avoiding reputational damage and financial penalties. In the case of non-compliance, online safety regulators could impose fines of up to 10% of qualifying worldwide revenue in the UK and 6% of global turnover in the EU.

Key themes arising from a cross-jurisdictional regulatory analysis

01 Age assurance requirements remain fragmented across Europe

- Online age assurance requirements exist in all countries analysed, but their stringency varies.
- Six jurisdictions – the **UK, France, Germany, Ireland, Italy and Spain –** have complemented requirements by publishing official guidance or technical standards for age assurance.
- **EU Digital Services Act (DSA) Guidelines** open the door for Member States to set their own minimum age for service access. A number of EU countries, including **France, Belgium** and **Italy**, are discussing proposals to set a minimum age for social media access, which may increase regulatory fragmentation.

02 Services in scope vary by jurisdiction

- **EU DSA Guidelines** include age assurance among measures that online platforms posing medium to high risks to children should implement.
- At a national level, audiovisual media services and pornographic content providers are a main focus, subject to some form of age assurance duties **in all jurisdictions** analysed.
- The **UK** extends requirements to all user-to-user and search services, **Italy** to internet access services, while **Germany** has adopted a service-agnostic approach.

03 Countries set different ages of consent for data processing

- The age of consent for data processing has been set to 13 in the **UK**.
- In the EU, it varies between 13 and 16, depending on the threshold set by each **EU** Member State under GDPR. These differences increase fragmentation, complicating cross-border compliance.

04 A risk-based approach is a common regulatory expectation

- Following **EU DSA Guidelines**, age assurance measures should be informed by a 'risk review'.
- At a national level, the **UK, Belgium, Ireland, Netherlands** and **Spain** emphasise taking a risk-based approach. This means that age assurance should be proportionate to the service's content, features, and user risk profile.
- In the **UK**, regulated services must complete annual risk assessments which should inform their age assurance strategies.

05 Privacy-preserving approaches are emerging as a baseline

- At **EU** level, DSA Guidelines emphasise compliance with data protection principles, particularly data minimisation, and *encourage* adoption of double-blind age methods ('double anonymity').
- At a national level, **France** and **Italy** go further, requiring the use of double anonymity for services hosting pornographic content. **Italy** also considers as non-compliant (with respect to privacy) systems based on the direct collection of IDs by pornographic sites; age estimation based on web browsing history; and the use of biometric data to identify or authenticate persons.

06 Services may choose different age assurance methods but will be responsible for ensuring their compliance and effectiveness

- No jurisdiction mandates specific technologies, leaving services some flexibility in their choice of age assurance approach. However, responsibility for the effectiveness and compliance of age assurance methods remains with the regulated service provider.
- Additionally, self-declaration approaches are considered insufficient across jurisdictions analysed. **Italy** and **France** go further, requiring age checks to access services hosting pornography to be performed by independent third parties. As mentioned above, these countries also makes clear that certain methods are overly privacy intrusive and thus non-compliant.

07 Age assurance as the foundation of age-appropriate design

- Under the **EU DSA** and in the **UK**, platforms are expected to mitigate the risk of harm across the user journey, requiring action beyond age assurance.
- Some Member States have called for new rules on mandated age-appropriate design, which would require companies to minimise addictive and persuasive service architecture (e.g. video autoplay, endless scroll).

08 We identify 11 cross-jurisdictional criteria relevant to implementation methods

- Regulators most commonly assess age assurance methods based on their accuracy, robustness, reliability, and non-discrimination.
- Additional criteria include non-intrusiveness, accessibility, complaints handling and anonymity.
- These criteria are outlined on the following page.

Common criteria guiding age assurance implementation

To be considered effective under EU DSA Guidelines and most official guidance at a national level [1], age assurance methods should be accurate, robust, reliable and non-discriminatory. In some jurisdictions, regulators also expect methods to be non-intrusive, accessible, and to provide clear complaints mechanisms to users. More stringent requirements may apply depending on a service's content and risk level. For instance, in Italy and France, technical standards for services disseminating pornography also mandate double anonymity, separation of duties and session-based verification.

01. Accuracy
Accuracy is flagged in **EU DSA** Guidelines and in national age assurance guidance in the **UK, France, Germany, Italy, Ireland**, the **Netherlands** and **Spain**. This reflects expectations that age assurance must be technically sound and assessed against appropriate metrics.

02. Robustness
According to the **EU DSA** Guidelines and national guidance in the **UK, France, Germany, Italy, Ireland**, the **Netherlands** and **Spain**, methods should actively resist circumvention attempts.

03. Reliability
Reliability is emphasised in **EU DSA** Guidelines and by national guidance in the **UK, France, Germany, Italy** and **Ireland**. This relates to the age output from an age assurance method being reproducible and derived from trustworthy evidence.

04. Fairness / Non-discrimination
According to the **EU DSA** Guidelines and national guidance in the **UK, France, Germany, Italy**, the **Netherlands** and **Spain**, regulated firms should ensure that age assurance methods do not result in discrimination (e.g., based on the ethnicity, disability or gender of the user).

05. Non-intrusiveness / Proportionality
Ensuring that users' rights are not disproportionately restricted when implementing age assurance measures is emphasised in **EU DSA** Guidelines as well as in national guidance in the **UK, France, Ireland, Italy** and **Spain**.

06. Complaints Handling
EU DSA Guidelines, **France, Germany, Ireland** and **Italy** specify that regulated services should provide mechanisms for users to challenge age assurance outcomes. In the **UK**, the ICO also expects decisions to be challengeable, whilst Ofcom is consulting on the topic.

07. Accessibility
EU DSA Guidelines flag the importance of ensuring accessibility. This is an explicit requirement in age assurance guidance in **Italy** and **Germany**. Accessibility is also explicitly linked to age assurance effectiveness in guidance issued in the **UK** and **Ireland**.

08. Anonymity
Double-blind methods are encouraged in **EU DSA** Guidelines and required by technical standards for services disseminating pornography in **Italy** and **France**. Non-binding guidance in **Spain** also calls for the use of methods that maintain user anonymity.

09. Interoperability / Portability
Encouraged at **EU** level via the Age Verification App and EUDI Wallet, as well as in national guidance in the **UK**. Alignment with the EUDI Wallet is also emphasised in the draft Organic Law in **Spain**.

10. Separation of Duties
EU DSA Guidelines specify that ID-based age verification should be performed by an independent third party. **France** and **Italy** require legal and technical separation between the age verification provider and services disseminating pornographic content.

11. Session-Based Verification
EU DSA Guidelines recommend that adult-only online platforms should conduct age assurance at each instance when their service is accessed. This is a binding requirement in **France** and **Italy** for services disseminating pornographic content.

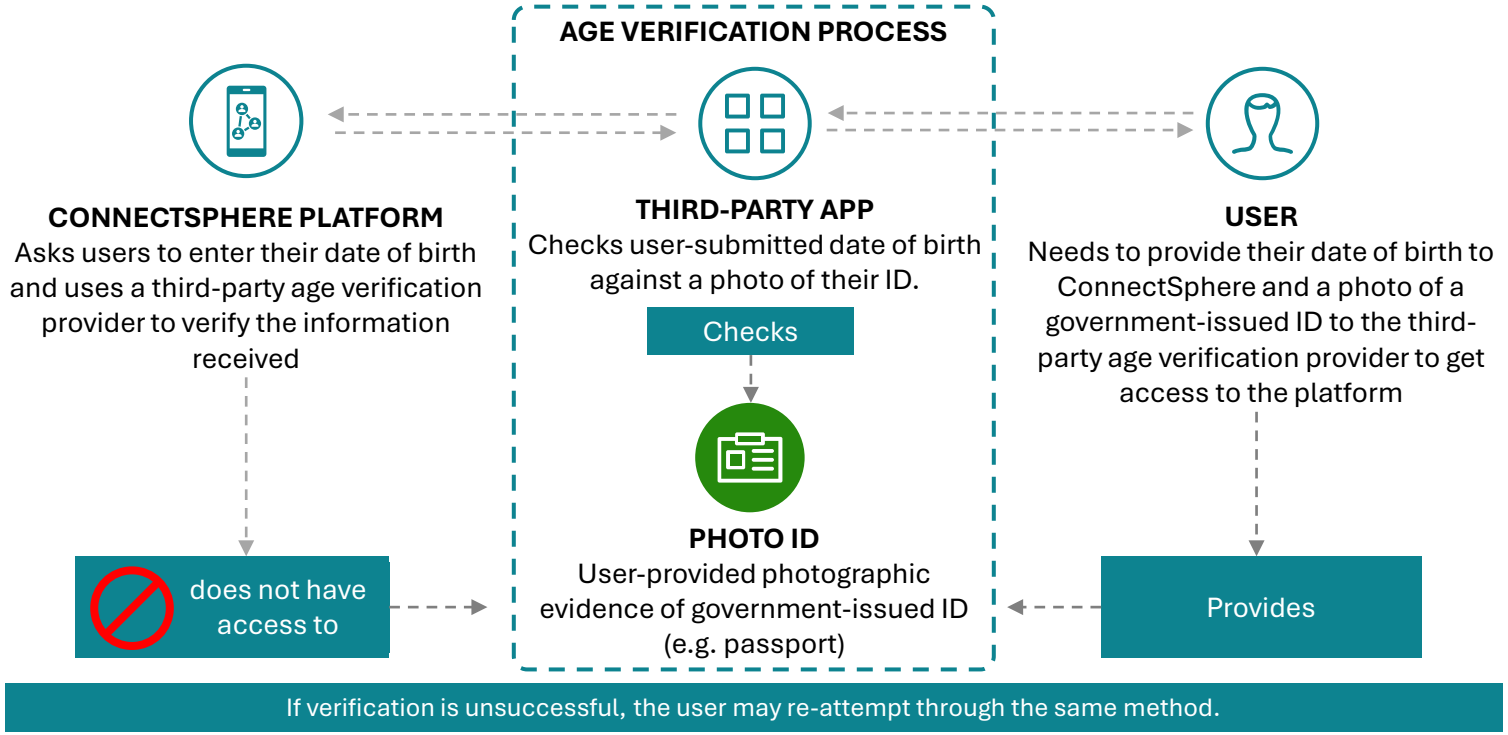
[1] Based on our analysis of regulatory requirements effective as of August 2025. This analysis focused on local criteria going above and beyond cross-European regulation such as GDPR. Please note that the scope of national guidance and standards varies, affecting the criteria's relevance for a given service. Further detail on relevant guidance and standards is available in Section 3. Please see Section 4 for definitions of each of these criteria.

Case study 1: implementing age assurance methods

ConnectSphere – Fictional social media company

While several methods may be capable of delivering effective age assurance, their appropriateness will vary depending on service-specific risks, applicable national requirements, and how the method is implemented. The following case study illustrates factors a fictional firm should consider in designing an age assurance process that meets regulatory expectations across markets.

- **Service:** ConnectSphere is a social media platform allowing users to share photos, videos and interact with each other. It is based in the UK and operates across Europe.
- **Status:** Based on its risk assessment under the UK Online Safety Act, ConnectSphere has introduced age checks to tailor children's experience when using certain high-risk features, such as direct messaging and live streaming. It now plans to roll out this approach across the EU.



Initial Considerations

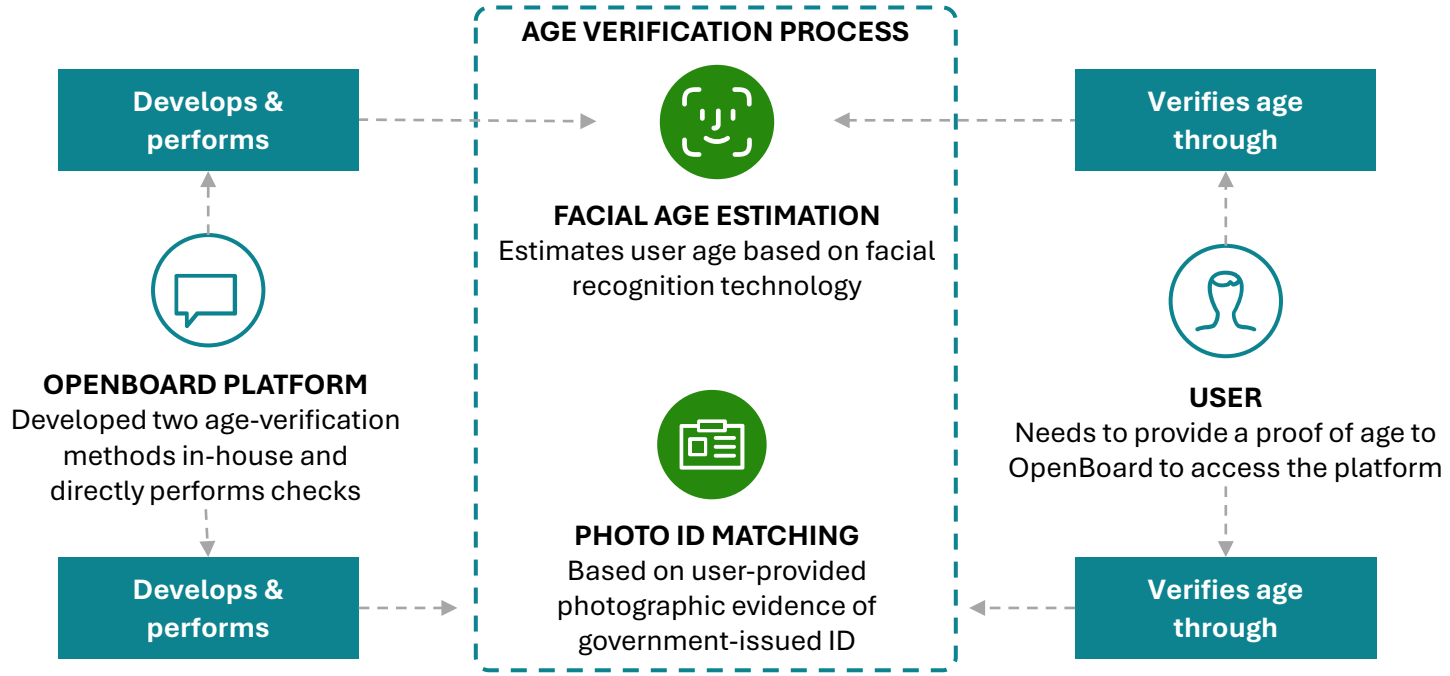
- Photo-identification matching is an age assurance method that Ofcom indicates is capable of being highly effective. In order to be considered highly effective, ConnectSphere should ensure its approach is **technically accurate, robust, reliable** and **fair**.
- Before rolling out its approach across the EU, ConnectSphere should also consider whether it aligns with the EU DSA, drawing on the Commission's Guidelines. The following points may be relevant:
  - The Guidelines note that **more than one age assurance method** should be offered. In the case of ConnectSphere, this may help ensure that users who lack access to government-issued IDs are not inadvertently excluded.
  - The Guidelines highlight the need for **non-intrusiveness**. To ensure compliance, ConnectSphere could consider alignment with the standards set by the EU age verification app. For example, it could accept a token of age from the third-party app, without requesting additional personal data such as the user's date of birth.
  - The Guidelines note that a **redress mechanism** should be provided for users to complain about incorrect age assessments. ConnectSphere could consider integrating this mechanism into its internal complaints-handling system.

Case study 2: implementing age assurance methods

OpenBoard – Fictional online forum

While several methods may be capable of delivering effective age assurance, their appropriateness will vary depending on service-specific risks, applicable national requirements, and how the method is implemented. The following case study illustrates factors a fictional firm should consider in designing an age assurance process that meets regulatory expectations across markets.

- **Service:** OpenBoard is an online forum hosting discussions across a range of interest-based communities. It is based in the Netherlands but is also popular in the UK and Italy.
- **Status:** Whilst not its primary purpose, OpenBoard's terms and conditions do not prohibit adult-only content from being uploaded and therefore restrict the use of the service to users over the age of 18 years old. As a result, it has determined that it should implement effective age assurance to prevent minors from accessing the platform.



Initial Considerations

- Both facial age estimation and photo-ID matching are age assurance methods that Ofcom considers capable of being highly effective. In implementing them, OpenBoard should ensure its approach is **technically accurate, robust, reliable** and **fair**.
- Given OpenBoard operates in the EU, it should also consider whether its approach aligns with the EU DSA, drawing on the Commission's Guidelines. In particular, the Guidelines specify that **ID-based age verification** should be based on anonymised age tokens issued by **independent third parties**, rather than the platform itself, particularly if it offers access to adult content. Additionally, **age estimation approaches** may not be considered appropriate and proportionate safeguards for services designed for an 18+ audience.
- Given it operates in Italy, if OpenBoard is disseminating pornographic content, it should also consider AGCOM's technical standards. The standards note that the processing of biometric data to identify the user during photo-ID matching and the direct collection of IDs by the platform is **overly privacy intrusive and non-compliant**. The standards require that the entity verifying age must **be legally and technically independent** from the content provider. Additionally, methods must maintain **double anonymity**, and users' age must be verified at **each session of service use**.

Section 2

Operational and strategic implications

02

Operational implications

Priority actions firms should consider

Building on the key themes and implementation criteria identified in the previous section, we translate findings from the cross-country analysis of regulatory requirements into a set of operational actions for service providers. These recommendations aim to help firms strengthen compliance, enhance method effectiveness and future-proof their age assurance approach.

Develop a centralised compliance tracker and effective early warning system

- Map current and emerging requirements across the jurisdictions in which the service operates or intends to expand into.
- Develop an early warning system underpinned by external regulatory, policy and political engagement where required.

Implement age assurance systems that are proportionate to service risks

- Conduct risk assessments to evaluate risks related to service content, features, user base, and algorithms – including legal but harmful content.
- Findings from risk assessments should inform the degree of assurance required, e.g., high-certainty age verification for high-risk services; age estimation for lower-risk services.

Balance safety with privacy-by-design

- Seek to secure privacy through data minimisation. In particular, consider aligning with emerging privacy-preserving methods, e.g. Zero-Knowledge Proofs and double-blind methods.
- Conduct a Data Protection Impact Assessment (DPIA), consider consulting young people and conducting a Child Rights Impact Assessment (CRIA) before implementing a solution.
- Prioritise solutions certified by relevant authorities or against international privacy standards.

Maximise accuracy, reliability and robustness

- Adopt evidence-based KPIs, such as false positives, completion rates and drop-off rates. Consider developing internal dashboards to track KPIs.
- Conduct comprehensive testing and implement robust anti-spoofing and anti-circumvention measures such as liveness detection.
- Consider ensuring alignment with emerging international standards (e.g. IEEE 2089.1 and the draft ISO/IEC 27566).

Ensure a non-discriminatory and accessible age assurance process.

- If relying on AI systems, ensure these are trained on a diverse data set to avoid biased outcomes.
- Offer a choice of age assurance methods to accommodate users with diverse needs.
- Provide complaints and redress mechanisms, allowing users to appeal age assurance outcomes.
- Ensure communications with users is clear and accessible. Consider tailoring language to different age groups.

Decide who should perform the age checks, and when they are performed

- Conduct a cost-benefit analysis of developing age assurance systems in-house vs third-party integration. In some jurisdictions, third-party provision is mandated.
- Consider prioritising providers certified by national authorities or against relevant standards.
- Determine when in the customer journey age checks should be performed, considering applicable regulatory requirements such as session-based verification.

Strategic implications

Priority actions firms should consider

Beyond operational actions, there are broader strategic implications that may influence a firms' approach to online age assurance. Differing regulatory requirements, evolving digital identity ecosystems, and increasing scrutiny of age-appropriate design have the potential to shape market entry decisions, future compliance strategies and product development. Here, we outline three strategic areas firms should evaluate as they navigate this rapidly evolving regulatory landscape.

Evaluate Geographic Footprint

- Companies should **evaluate their geographic footprint** in light of divergent regulatory requirements and userbase distribution.
- For some firms, the cost of implementing robust systems may influence **decisions on how and where services are offered**, for instance, when to launch a new product or functionality in a new market.
- Other firms may **consider opting to align with the most stringent standards** available to ensure long-term compliance should other countries step up their regulatory ambition.

Future-proof Age Assurance Strategy

- Given expected rollout of EU Digital Identity Wallets and the GOV.UK Wallet, firms should consider **ensuring their approach can integrate with digital identity ecosystems**.
- This could shape long-term decisions around age assurance architecture, vendor selection, and data governance. In particular, the implementation of the reference standard set by the EU age verification app points to **privacy-preserving, data-minimising, non-traceable** and **interoperable technologies**.
- Firms should **consider participating in available trials of the EU age verification app and EUDI Wallets**. This may provide valuable insights into how to future proof compliance strategies. However the app's initial focus will be on verifying if users are 18+, so will not be able to help in identifying the age of younger users for the purposes of offering age-appropriate content, at least initially.
- **Aligning with EUDI Wallets** may have implications beyond age assurance, for example allowing users to sign up and securely authenticate who they are upon service access.

Integrate Age Assurance Into Product Development And Age-appropriate Design

- For many services, **age assurance will be necessary to ensure young users do not access risky service features or content categories**, rather than simply blocking access entirely. This carries strategic service design implications.
- One option would be a **tiered service model**, using age assurance to tailor content, features, and settings based on a user's age group. For example, a social media platform may consider turning off ephemeral design features (e.g. streaks) and setting accounts to private-by-default for users under 18. Additional changes may be necessary for younger age groups (e.g. 13 – 16). Risk assessments can inform these design choices by identifying how different age groups may be exposed to – and affected by – different risks.
- More generally, firms should **anticipate greater regulatory scrutiny of service design** and be prepared to demonstrate how risks related to design features (from user interfaces to algorithmic recommendations) are mitigated, which may further impact service design in the future.

Breaking silos

The importance of collaboration across teams

Implementing effective age assurance processes is not solely a responsibility for Trust and Safety professionals. It requires a coordinated effort across the organisation. Specialist teams should collaborate and secure buy-in from decision makers within the firm to ensure solutions are compliant, effective, and feasible to implement. Expanding on the operational and strategic implications set out earlier in this report, the actions below outline indicative responsibilities for common business areas, which will vary depending on organisational structure, scale, and the company's chosen approach to age assurance.

Legal

- **Keep track of current and emerging age assurance regulations** across operating and target markets.
- **Embed age assurance compliance checks into third party contract templates**, ensuring suppliers meet technical and legal benchmarks.
- **Conduct DPIAs** before implementing any kind of age assurance process.
- **Audit vendors** on GDPR Art. 28 requirements and other national privacy requirements.

Trust & Safety

- **Conduct regular risk assessments** to calibrate age assurance based on service risks.
- **Track and incorporate age assurance KPIs** into internal reporting and enterprise risk dashboards.
- Monitor and advocate for **age-appropriate design**.
- Appoint a **senior accountable person** to liaise with regulators, seeking proactive engagement.
- **Provide timely and accurate responses** to formal information requests from regulators.

Business development / Partnerships

- **Identify and assess third-party providers** certified against relevant national or international standards.
- Negotiate agreements that **ensure third-party providers meet applicable regulatory requirements**.
- **Explore cross-industry collaborations and pilot projects** to trial emerging solutions (e.g., EU age verification app pilots).

Technology & Engineering

- Build APIs or modular infrastructure that **enable plug-and-play integration with certified third-party age verification providers.**
- **Incorporate protocols and design standards** for privacy-preserving tokenisation and session-based architecture where relevant.
- **Develop internal test environments** to simulate real-world effectiveness (e.g. error rates, session duration, fallback protocols).

Product

- **Integrate age assurance into product design,** applying differentiated protocols by product type (e.g. to access live streaming, comments, direct messaging).
- Seek to **minimise friction and improve the user journey** associated with age verification processes.
- Ensure **redress and appeals processes** are in place.
- Collaborate with legal and technology teams to **test designs compatible with the EUDI Wallet, the EU age verification app, or other token-based ID systems.**

Communications / Marketing

- **Develop user-friendly public communications** explaining why and how age checks are conducted,
- **Create educational campaigns and FAQs** that explain the safety benefits of age assurance, strengthening user trust and acceptance of age assurance processes.
- **Monitor public sentiment and competitor positioning** on age assurance to inform brand strategy and reduce reputational risks.

Section 3

Navigating age assurance requirements under specific European jurisdictions

The following pages summarise key regulations and initiatives, as of August 2025, relevant to online age assurance in the UK, the EU and seven EU Member States: Belgium, France, Germany, Ireland, Italy, Netherlands and Spain

03

United Kingdom

Key age assurance regulations and initiatives

Summary

UK online age assurance regulation is primarily governed by the Online Safety Act (OSA), requiring Highly Effective Age Assurance (HEAA) for platforms hosting certain types of harmful content. Ofcom, the UK's communications regulator, enforces the OSA regime, with potential penalties for non-compliance up to £18 million or 10% of qualifying worldwide revenue. HEAA must be technically accurate, robust, reliable, and fair, according to Ofcom's guidance on HEAA. Data protection principles must also be integrated, emphasising data minimisation and data protection by design within the chosen HEAA method.

Regulatory developments

Current Regulations and Guidance	• **Online Safety Act (OSA):** Mandates HEAA for platforms hosting certain types of content. Age assurance duties for services that display or publish their own pornographic content took effect on 17 January 2025. Since 25 July 2025, assurance duties also apply to regulated user-to-user and search services likely to be accessed by children that allow primary priority content (pornography, suicide, self-harm and eating disorder content) or priority content, as well as services with a content recommender system that pose a risk of primary priority content/priority content/non-designated content. • **Ofcom's Guidance on HEAA:** Details age assurance expectations for services in scope relevant duties under the OSA. • **Video-Sharing Platform (VSP) regime:** The VSP regime, which ran for four years, was repealed on 25 July 2025, with all notified services now regulated under the OSA. • **UK GDPR:** The age of consent for personal data processing is set at 13 years old. • **Information Commissioner's Office (ICO)'s Code and Opinion on Age Assurance:** Sets out its expectation for age assurance and children's data protection, emphasising data minimisation, non-intrusiveness and a risk-based approach. • **ICO Trademark:** Recently developed by the ICO, it provides an endorsement of the quality and assurance provided by owners of ICO approved and published UK GDPR certification schemes (including for age assurance solutions).
Enforcement	• **Ofcom** is responsible for enforcing the OSA regime. Non-compliance may lead to fines up to £18 million or 10% of qualifying worldwide revenue (whichever is higher), as well as business disruption measures.
Emerging Regulations and Initiatives	• **Additional Safety Measures Consultation:** Open until 20 October 2025, it sets out Ofcom's proposals to strengthen the Codes of Practice under the OSA. Proposals include expanding requirements to implement HEAA measures, particularly to restrict high-risk features like livestreams, and the requirement to have age assurance appeals mechanisms for users to challenge outcomes. • **Ofcom age assurance report**: Ofcom plans to develop a report on the use of age assurance, with expected publication in 2026. • **Categorised services regime:** Additional duties will be announced for the largest "categorised" online services, including identity verification (which is not the same as age assurance, but is related) for services designated as Category 1.

Guidance on HEAA - Key considerations

- **Data protection by design:** Services must ensure compliance with both the OSA and the data protection regime overseen by the ICO. They should follow a "data protection by design" approach and consult ICO guidance, including its Opinion on Age Assurance.
- **Technology neutrality:** Flexibility in method, so long as they comply with Ofcom's criteria.

Ofcom laid out **four criteria** that should be fulfilled to ensure an AA process is highly effective:

1. **Accuracy**: The method can correctly establish whether or not a particular user is a child. Some metrics to measure technical accuracy are suggested in Ofcom's guidance.
2. **Robustness**: The method has undergone testing under different conditions and mitigations are in place against circumvention attempts. Service providers should not publish content encouraging users to bypass age assurance, such as by promoting VPNs.
3. **Reliability**: The output is reproducible and derived from trustworthy evidence.
4. **Fairness**: It avoids or minimises bias and discriminatory outcomes.

Whether outsourcing to a third-party provider or not, it is still the service's responsibility to ensure that the age assurance process meets all the above criteria.

When implementing an age assurance method, companies should also have regard to:

- **Accessibility**: Ensuring it is easy to use for all users regardless of their characteristics.
- **Interoperability**: Ensuring the method is easy to use and access across devices.

Ofcom provides a non-exhaustive list of **seven methods capable (though not guaranteed) of being highly effective**: Credit card checks, open banking, photo-ID matching, facial age estimation, MNO age checks, digital ID services and email-based age estimation. Ofcom flags **three methods incapable of being highly effective**: self-declaration, age verification via payment methods that don't require to be 18+, and general contractual restrictions on use by children.

European Union

Key age assurance regulations and EU-wide initiatives

Summary

The EU's regulatory framework for age assurance is largely based on the Digital Services Act (DSA), the Audiovisual Media Services Directive (AVMSD), and the General Data Protection Regulation (GDPR). Effectively responding requires careful consideration of proportionality, risk assessments, and user privacy. The European Commission (EC) has also developed a white label age verification app to assist compliance with the DSA. In addition, it will be rolling out the EU Digital Identity (EUDI) Wallet in each Member State, incorporating an age verification functionality. The roll-out is expected to be finalised by the end of 2026.

Regulatory developments

Current Regulations and Guidance	• **DSA:** Art. 28 imposes broad obligations on online platforms to implement "*appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors, on their service*". Age assurance is not mentioned, but the article enables the Commission to issue guidelines, which it has done. • **AVMSD:** Audiovisual media services (broadcast, on-demand and VSPs) must take "*appropriate and proportionate measures*" to protect minors from content that may impair their physical, mental, or moral development (e.g., pornography, gratuitous violence, self-harm). This may include age verification systems, where appropriate. As a Directive, the AVMSD has been transposed into national law in each national jurisdiction. It is due to be reviewed in 2026. • **GDPR:** Art. 8 requires parental consent for processing the data of children under a certain age, set between 13 and 16 by each Member State (MS). This applies across the European Union. Whilst not legally binding, the **EDPB's statement on age assurance** outlines ten principles for GDPR-compliant age assurance.
Enforcement	• **DSA**: The **EC** (regarding VLOPs and VLOSEs) and **Digital Service Coordinators** (DSCs) (regarding in-scope services at Member State level). DSC activity under the DSA relevant to age assurance has been limited to date. The DSA states that fines issued for non-compliance may reach up to 6% of global turnover. • **AVMSD**: Enforced by national regulators, with penalties and oversight varying by Member State but coordinated at EU level by the European Commission. • **GDPR**: Enforcement relies on national data protection authorities and EU-wide cooperation. Fines for minors-related data breaches may reach up to €20 million or 4% of global annual turnover.
Emerging Regulations and Initiatives	• **EU white label age verification app**: The EU is currently testing an EU-wide age verification app which will provide a reference standard for age verification before EUDI Wallets become available. • **EU code of conduct on age-appropriate design**: Under the BIK+ strategy, the Commission will facilitate a comprehensive EU Code of conduct on age-appropriate design ('BIK+ Code'). • **EU Digital Fairness Act:** Seeks to address harmful online practices such as dark patterns, addictive design and profiling to protect consumers, including minors. Currently expected Q3 2026.

Key considerations

The EU Digital Identity Wallet

- Is intended to provide a safe, reliable, and private means of electronic identification in the EU.
- Every MS is required to provide at least one wallet by the end of 2026.
- Wallets will embed the opportunity to receive a **token of age** from issuing services, allowing to verify age without disclosing any other personal data.

DSA Guidelines (detailed overview on the next page)

- **Age verification**: Suitable when required by EU or national law (including minimum age to access social media), for adult-only services, where terms and conditions require users to be 18+, or when high, unmitigated risks to minors are identified in the risk assessment.
- **Age estimation**: Suitable when the terms and conditions specify a minimum age under 18 or when medium risks are identified in the risk assessment.
- **Five criteria**: Effective age assurance methods must be accurate, reliable, robust, non-intrusive, and non-discriminatory.
- A **joint letter** signed on 18 June 2025 by eleven EU Member States (including France, Ireland, Italy and Spain) has urged the Commission to consider mandatory age verification for access to social media platforms as "*an indispensable and appropriate measure in view of the risks involved*". This signals Member States' ambition to go beyond the DSA Guidelines, suggesting the potential for a shift towards stricter enforcement of DSA Art. 28.

EU DSA Guidelines on the Protection of Minors Online

Age assurance to restrict access to adult content, or when national rules set a minimum age

Summary

On 14 July 2025, the European Commission published non-binding guidelines on the protection of minors under the Digital Services Act (DSA), along with an age verification blueprint. The guidelines provide recommendations to ensure high levels of privacy, safety and security for children on online platforms. The guidelines outline when and how platforms should check users' age. They recommend age verification for adult content platforms and other platforms that pose high risks to the safety of minors. They specify that age assurance methods should be accurate, reliable, robust, non-intrusive and non-discriminatory.

Age assurance guidance

When should age checks be performed	• **Age verification:** Suitable for high-risk services; where terms and conditions require users to be 18+; where high, unmitigated risks to minors have been identified in the risk assessment; or where EU or national law mandates a minimum age to access certain products or services (e.g. minimum age to access social media). • **Age estimation:** Suitable where the terms and conditions specify a minimum age under 18 or where medium risks are identified. Age estimation can be used as a transitory measure where effective age verification solutions are not yet readily available[1]. • **Beyond restricting minors' access:** Age assurance can be used to prevent adults from accessing services designed for children only (except when access is legitimate). It can also be used to underpin the age-appropriate design of a service, tailoring access to content, features and activities to a child's age.
Five criteria	The Guidelines outline **five criteria** that should be used to assess the appropriateness and proportionality of any age assurance method: 1. **Accuracy**: The method should accurately determine whether a user is above or below a certain age, or the user's age range. 2. **Reliability**: It works well in real-world circumstances and uses reliable data. 3. **Robustness**: It should not be easy to circumvent and should be secure. 4. **Non-intrusiveness**: It should not be intrusive on users' rights and freedoms. 5. **Non-discrimination**: It should not discriminate against some users. It should be appropriate and available for all minors, regardless of disability, language, ethnic, gender, religious and minority backgrounds.

Key considerations

- **Risk-based approach:** Safety measures must be proportionate to risk and must not unduly restrict children's rights. Platforms should always conduct a risk assessment to determine whether age assurance is appropriate. Risk assessments should be made publicly available.
- **Transparency**: Platforms should provide information on the age assurance solutions adopted, their adequacy and performance metrics (e.g. false positives) to evidence their effectiveness.
- **Data protection**: Guidelines emphasise compliance with GDPR principles, particularly data minimisation, and encourage platforms to consider the EDPB statement on age assurance.
- **Double anonymity:** To ensure compliance with the principles of data minimisation, purpose limitation, and user trust, services are encouraged to adopt *double-blind* age verification methods.
- **Age verification using government IDs** should be based on anonymised age tokens issued by **independent third parties**, particularly where the service provider offers adult content.
- **Targeted restrictions**: Some online platforms (e.g., social media) should implement age-appropriate access restrictions on risky content, sections, or functions, rather than blocking the entire platform. Age verification should be used to enforce these restrictions.
- **Multiple methods**: Platforms should offer at least two age assurance methods.
- **Redress**: Platforms should provide a redress mechanism to users to challenge outcomes.
- **Self-declaration**: Considered inappropriate as it lacks accuracy, reliability and robustness.
- **Children should be involved** in the design and evaluation of age assurance methods.
- **Session-based verification**: Adult-only services should not allow sharing of user account credentials and thus conduct age assurance at each instance when their service is accessed.
- **Third party use**: to carry out age assurance should be explained in child-friendly language. Ultimately, the company remains responsible for ensuring the third-party method is effective.

EU White Label Age Verification App

Intended to be a harmonised, privacy-preserving age verification solution for the EU

Summary

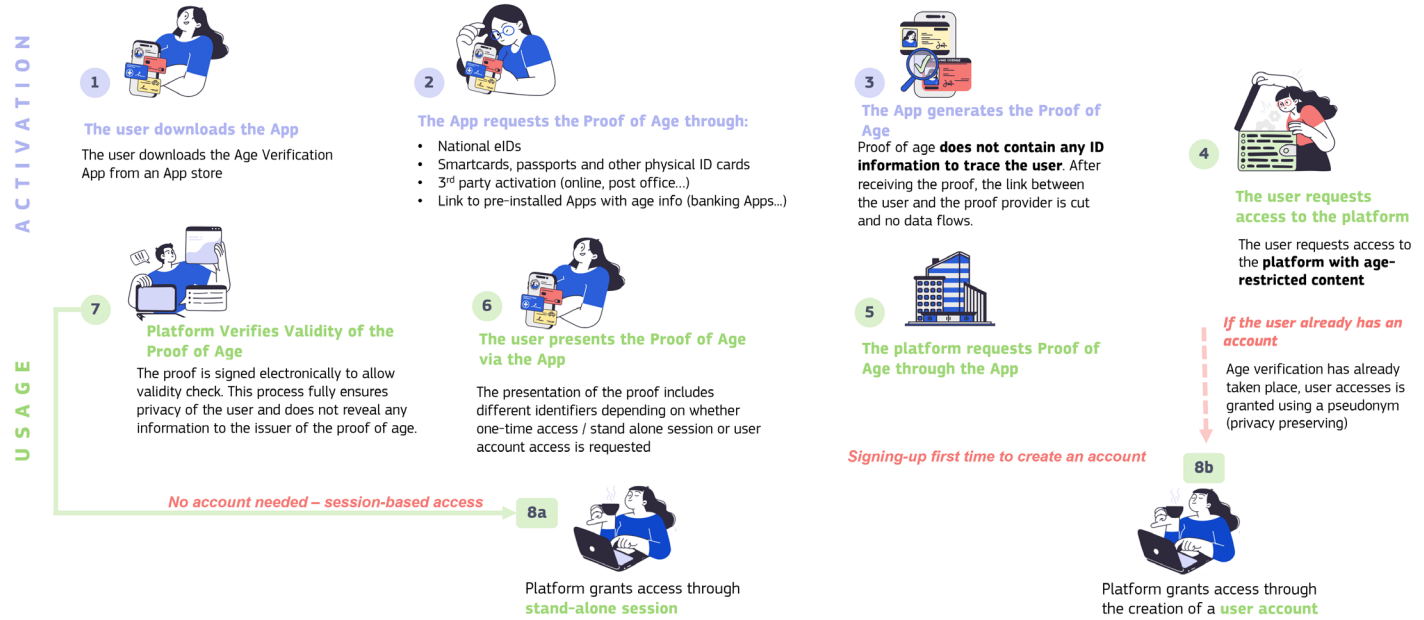
The EU has developed a white label age verification solution, operationalising compliance with Article 28 of the DSA. This aims to provide a user-friendly and privacy-preserving solution, setting a "gold standard" and compliance benchmark for age assurance online. It is designed to work across all Member States and is built on the European Digital Identity (EUDI) Wallet framework. It is intended to bridge the gap until EUDI Wallets become available by the end of 2026. Once deployed, EUDI Wallets will allow users to verify their age by sharing only specific information (e.g. being 18+) with a service.

- **Current status and timeline**: A prototype of the app has been released on 14 July 2025, alongside the final DSA Guidelines. The app is being tested and further customised in collaboration with Member States, online platforms and end-users. Open-source technical specifications, providing details on the app's design, have been published on the app's dedicated website.
- **Member State deployment**: Denmark, Greece, Spain, France and Italy, identified as frontrunners, will be the first to engage with the Commission on the technical solution with the aim of launching national age verification apps. The prototype can be integrated into a national app or remain a free-standing app. Each Member State will be responsible for publishing their country specific app in their local app stores.

Main features of the app

- **Privacy-preserving**: The app will use a proof of age to allow users to verify they are over 18 to access age-restricted services, without revealing other personal data such as the user's exact age or identity. Additionally, tracking across platforms will be prevented.
- **Device-based**: The proof of age will be stored on mobile devices (phones/tablets). This may result in risks where device are shared, and mitigating measures are under consideration.
- **Double anonymity**: The trusted proof provider is not informed about which online services the user seeks to access. Likewise, 18+ online service providers do not receive the identity of the user requesting access, only a proof that the user is 18 or older.
- **Interoperability**: The app is designed for seamless integration across various devices, operating systems, and online services. It will rely on existing standards (OpenID4VCI and ISO/IEC 18013-5).
- **Equity**: The app is designed to be accessible and inclusive. To support inclusivity, the proof of age can be requested in several different ways.
- **Initial use case**: At first, the app's focus will be on verifying if users are over 18 to allow for swifter deployment. Other use cases that Member States could pursue may include enforcing national restrictions for social media use set at different age thresholds.

User journey on the age verification app (e.g. 18+)



Source: Operational, Security, Product and Architecture Specifications

France

Key age assurance regulations and initiatives

Summary

France has emerged as one of the most ambitious EU countries on age assurance regulation, going beyond transposition of the AVMSD. Under the SREN Law (Loi sur la Sécurisation et la Régulation de l'Espace Numérique), France has implemented age assurance duties for platforms hosting pornographic content, which includes technical standards for age verification systems. In addition, Law no. 2023-566 has introduced a digital age of majority at 15, requiring parental consent for social media access by younger users. More recently, France has tabled a proposal to establish an EU-wide digital age of majority. On 16 June 2025, a Paris Administrative Court ruling suspended age verification for pornographic companies based in other EU member states. A final judgment reinstated this requirement on 16 July 2025.

Regulatory developments

Current Regulations and Guidance	• **SREN Law:** Imposed requirements on all platforms hosting pornographic content requiring **them to** implement age verification systems (AVS). From 7 June 2025 this was extended to platforms based in other EU Member States. • **Arcom Standard: Arcom (the French authority for audiovisual and digital communication) published technical standards detailing the minimum AVS effectiveness requirements that regulated services must meet.** • **Law no. 2023-566:** Introduces a digital age of majority at 15, requiring parental consent for social media access by younger users. To date, implementation **is pending, as France must ensure that this legislation complies with EU law.** • **GDPR: T**he age of consent for personal data processing is set at 15 in France. • **The CNIL has set out non-binding recommendations on approaches to "verify the age of the child and parental consent, while respecting the child's privacy"**
Enforcement	• **Arcom** oversees the enforcement of SREN Law and can request compliance audits to be carried out by independent organisations. In case of non-compliance, Arcom can impose fines up to €150,000 or 2% of global turnover (whichever is higher) and may order the blocking of non-compliant sites within 48 hours.
Emerging Regulations and Initiatives	• **EU-wide Digital Age of Majority Proposal**: On 16 May 2025, France, Greece, and Spain put forward a proposal to strengthen age verification duties and introduce a pan-European digital age of majority to access social media. • **Social media ban for children under 15**: In June 2025, President Macron stated he intends to ban social media access for children under 15 in France, unless more stringent EU measures are introduced, emphasising the urgency to act. • **June 2025 joint letter**: France is among the eleven signatories of the joint letter urged the Commission to consider mandatory verification for access to social media platforms as "*an indispensable and appropriate measure in view of the risks involved*". This signals France's ambition for stricter enforcement of Article 28 of the DSA. • **EU White Label Age Verification App**: France was one of five countries selected to beta test the EU white label age verification app.

Arcom Standard – Key considerations

- **Accuracy, reliability and robustness** : Arcom considers self-declaration as non-compliant. AVS must be accurate and must reliably differentiate minors from adults and should have robust anti-circumvention measures against spoofing attempts, including the use of deepfakes. To avoid bias, AVS should be trained on diverse data sets.
- **Separation of duties**: The entity verifying age must be legally and technically independent from the content provider.
- **Session-based verification**: Adult content providers must verify age at each session of service use (expiring automatically after 1 hour of inactivity).
- **Non-intrusiveness / Data minimisation**: AVS should not store personal data or official ID documents unless necessary for generating reusable proof of age.
- **Double anonymity**: The verification process must ensure that the content provider cannot identify the user, and the AVS provider does not know which service the user is accessing.
- **Non-discrimination**: The AVS should not lead to unequal treatment among users.
- **User complaints and transparency**: Users must have the ability to challenge age verification outcomes. Services must clearly inform users about the level of privacy protection and the methods used for age verification.

Belgium

Key age assurance regulations and initiatives

Summary

Belgium's approach to age assurance is currently evolving. Existing regulations primarily focus on audiovisual services, but there is growing political discussion around broader online safety for minors. The Flemish, French and German speaking Communities have transposed the EU AVMSD, while discussions are ongoing regarding stricter rules to regulate minors' social media use and related algorithmic recommendations. In this context, a ban on social media below the age of 16 years is under discussion, although its adoption remains uncertain due to significant opposition.

Regulatory developments

Current Regulations and Guidance	• **Flemish Media Decree (and French and German Community equivalent):** – Represents transposition of the AVMSD. Requires TV broadcasters to prevent minors from accessing harmful content. Age verification may be implemented to comply. – Extends similar obligations to video-sharing platforms, explicitly recognising age verification systems as an appropriate measure to comply. • **GDPR**: The age of consent for personal data processing is set at 13 under national law, requiring parental consent for younger children.
Enforcement	• The **Regulators (VRM, CSA and Medienrat)** oversee compliance with the Media Decrees, however, since age assurance is only one among several acceptable measures to comply with duties, its enforcement is limited.
Emerging Regulations and Initiatives	• **Drafting of a national minors protection law**: Following the publication of the EU DSA Guidelines in July 2025, the federal minister for digital matters Vanessa Matz called for the drafting of national legislation to enhance minors protection online, including mandatory requirements. Parliamentary debates are expected to commence shortly. • **Debate on social media regulation**: Ongoing discussions about stricter age verification requirements for social media access, with a social media ban until the age of 16 advocated by some experts. • **June 2025 joint letter**: The Wallonia-Brussels Federation is among the eleven signatories of the joint letter urging the Commission to consider mandatory verification for access to social media platforms as "*an indispensable and appropriate measure in view of the risks involved*". This signals an ambition for stricter enforcement of Article 28 of the DSA. • **Concept Note on Algorithmic Recommendation Systems (Flanders):** Submitted in January 2025 by seven members of the Flemish Parliament, it proposes an ethical framework for algorithmic recommendations targeting young people, including recommendations for robust age verification (e.g., biometric verification). The Concept Note is currently under parliamentary review. • **Resolution of 11 January 2024 on Protecting Children from Inappropriate Online Content:** This resolution from the Belgian Chamber of Representatives, while non-binding, advocates for a national coordinating body to implement the EU's Better Internet for Kids+ strategy. The resolution focuses on increasing accessibility to parental control systems, indirectly suggesting age verification as a potential tool within this framework. While age assurance isn't explicitly mentioned, its role in enhancing parental controls is implied.

Key considerations

- **Risk-based approach:** Under the Media Decrees, measures should be proportionate to the content's potential harm to children.
- **Technology neutrality**: Belgium adopts a technology-neutral approach, allowing flexibility in the choice of appropriate age assurance solutions.
- **Data protection:** GDPR principles (e.g. Lawfulness, Data Minimisation, Fairness, Purpose Limitation) apply. The Media Decrees also require that personal data of minors collected for the implementation of age verification shall not be processed for commercial purposes.
- **Accuracy and reliability**: The Concept Note (see Emerging Regulations and Initiatives) criticises existing age verification methods as inadequate since they rely on self-declaration or simple age limits that are easily circumvented. The Concept Note calls for more accurate and reliable solutions. Biometric verification, including facial recognition and fingerprint scanning, is proposed as offering a seamless and secure method of age verification.

Germany

Key age assurance regulations and initiatives

Summary

Germany has established age assurance requirements primarily through the Protection of Young Persons Act (JuSchG) and the Interstate Treaty on the Protection of Minors in the Media (JMStV), which is part of Germany's transposition of the AVMSD. These regulations mandate age verification for online access to content that is harmful to minors, and to age-restricted goods and services. Currently, the government is discussing introducing more stringent regulatory requirements to strengthen the protection of minors online, particularly on pornographic platforms.

Regulatory developments

Current Regulations and Guidance	• **JuSchG** (effective since May 2021): Requires all service providers to ensure that minors do not have access to harmful content. • **JMStV:** Requires all forms of electronic media to implement age verification "equivalent to face-to-face checks" to protect children from severely harmful content (e.g. pornography, glorification of violence). • **The Commission for the Protection of Minors in the Media (KJM) guidelines:** The KJM has published guidelines on age verification methods considered effective and suitable to meet legal requirements. The KJM also offers a certification procedure to certify age verification systems considered effective to meet legal duties. • **GDPR: T**he age of consent for personal data processing is set at 16 under national law, requiring parental consent for younger children. The Federal Commissioner for Data Protection and Freedom of Information (BfDI) and state data protection authorities collaborate with the KJM and other youth media protection bodies on an informal, non-officially obligated basis.
Enforcement	• While the **KJM** provides guidance, it is the responsibility of **state media authorities** and **data protection authorities** to enforce age assurance duties related to the JMStV, JuSchG, and GDPR and the Federal Data Protection Act (BDSG) respectively. Non-compliance can lead to fines (up to €500,000 under JMStV), site blockings, content removal and legal action.
Emerging Regulations and Initiatives	• Discussions are ongoing over further regulation of pornographic platforms. The government is examining additional measures to improve the protection of minors online through further legislation and/or funding programmes for technical developments.

KJM guidelines – Key considerations

- **Service-agnostic regulation**: Age verification duties in Germany do not target specific service providers. Rather, they apply based on the content and services offered.
- **Technology neutrality**: The JMStV requires "appropriate" and "effective" protective measures, leaving companies the choice of methods among those certified by KJM.
- **Data protection**: Compliance with all GDPR principles is mandated by KJM guidelines.
- **Effectiveness**: The KJM has developed specific test criteria for assessing the effectiveness of age verification and maintains a list of over 100 tools certified as effective. These include video-identification, AI-based ID checks, and document scans.
- **Non-compliant methods**: KJM considers self-declaration, non-validated registration data, and verification only by cookies among insufficient methods to fulfil duties.
- **Accuracy:** In the certification process, the KJM checks whether such errors are minimized by technical data redundancy and testing mechanisms.
- **Robustness**: Services must implement strict anti-circumvention measures.
- **Reliability:** Age verification outcomes must be reproducible and be based on trusted data sources, with a particular emphasis on traceability.
- **Non-discrimination**: Methods must not discriminate against users based on the device they use, their accessibility needs, ethnicity or any disability.
- **Accessibility**: Methods must be intuitive and easy to use for users of all age groups.
- **Complaints handling**: Users must be able to challenge age assurance outcomes.

Ireland

Key age assurance regulations and initiatives

Summary

National requirements in Ireland are primarily governed by the Online Safety Code (OLSC). It has introduced obligations on video-sharing platforms (VSPs) headquartered in Ireland to protect people, especially children, from harmful content. Irish media regulator, the Coimisiún na Meán (CnaM), has designated 9 VSPs that have to comply with OLSC. The Data Protection Commission (DPC) has been heavily involved in the regulatory process, seeking to strike a balance between online safety and data protection.

Regulatory developments

Current Regulations and Guidance	• **Online Safety Code (OLSC):** Developed under the **Online Safety and Media Regulation Act 2022, part of Ireland's transposition of the AVMSD.** The OLSC mandates the use of effective age assurance (which may include age estimation) for VSPs headquartered in Ireland whose terms and conditions do not preclude the uploading or sharing of harmful and adult-only content – defined as *"pornography and extreme or gratuitous violence"* (effective 21 July 2025). • **Online Safety Guidance:** CnaM lists some recommended characteristics for age assurance measures to be considered most effective. • **EDPB's statement on age assurance:** The DPC acted as a co-rapporteur. • **GDPR:** The age of consent for personal data processing is set at 16 under national law, requiring parental consent for younger children. • **"Fundamentals" for Children's Data Processing:** DPC-published guidance stating that online service providers should either treat all users as children by default or take a risk-based approach to age verification. Age verification must comply with data protection principles and be subject to Data Protection Impact Assessments.
Enforcement	• **CnaM** and **DPC** will both monitor the implementation of age assurance duties. Non-compliance with the OLSC can lead to fines up to €20 million or 10% of a platform's global annual turnover (whichever is greater). It may also lead to potential market restrictions and personal liability for senior executives.
Emerging Regulations and Initiatives	• **June 2025 joint letter:** Ireland is among the eleven signatories of the joint letter that urged the Commission to consider mandatory verification for access to social media platforms as "*an indispensable and appropriate measure in view of the risks involved*". This signals Ireland's ambition for stricter enforcement of Article 28 of the DSA.

OLSC – Key considerations

- **Technology neutrality:** Although CnaM does not specify the age assurance methods regulated services should use, self-declaration alone is explicitly considered insufficient. CnaM considers measures to be most effective when they meet some **recommended characteristics**, including:
- **Accuracy and robustness:** Accurately assure age and include protections against circumvention.
- **Non-intrusiveness:** Implemented proportionately to the harm caused by unrestricted access to content and not unduly limiting children's rightful access to quality content.
- **Non-discrimination:** operate consistently and fairly in respect of all users.
- **Data protection and privacy:** Age assurance must comply with all GDPR requirements.
- **Accessibility:** Measures should be easy to use, particularly for children, and accessible.
- **Industry standards:** Meet industry standards on quality parameters (no further specification).
- **Terms and Conditions:** Must include a requirement that users comply with and do not attempt to circumvent age assurance.
- **Complaints handling:** VSPs must establish and operate transparent, easy-to-use and effective procedures for handling user complaints.

Italy

Key age assurance regulations and initiatives

Summary

Italy has established age assurance requirements primarily through Legislative Decree 123/2023 and related AGCOM Resolution 96-25-CONS, focusing on pornographic content. The AGCOM technical specification for age verification systems (AVS) is considered among the most stringent in Europe. Other regulations (TUSMA) address VSPs and electronic communications, including parental controls. AGCOM plays a central role, with the Garante per la protezione dei dati personali (Italian Data Protection Authority) ensuring privacy compliance.

Regulatory developments

Current Regulations and Guidance	• **Legislative Decree 123/2023** and **Resolution 96-25-CONS** (effective 12 November 2025): Mandates age verification for websites and VSPs disseminating pornographic content. AGCOM has defined **the technical and procedural standards** that regulated services must follow for verifying age. • **TUSMA (Legislative Decree 208/2021):** TUSMA implements the EU AVMSD in Italy, requiring VSPs to implement measures to protect minors from harmful content, including age verification and parental controls. • **Legislative Decree 28/2020** and **Resolution 9/23/CONS**: Mandates parental control systems (PCS) for internet access services. PCS should filter inappropriate content or block underage access to adult material. • **GDPR:** The age of consent for personal data processing is set at 14 under national law, requiring parental consent for younger children.
Enforcement	• **AGCOM** is responsible for enforcement of Decree 123/2023. Non-compliance can lead to fines from €10,000 to €260,000, as well as website blocking. • **AGCOM** is responsible for TUSMA, violations can lead to fines from €30,000 to €600,000 or 1% of the annual turnover generated in Italy (whichever is higher), as well as content restriction.
Emerging Regulations and Initiatives	• **June 2025 joint letter**: Italy is among the eleven signatories of the joint letter urged the Commission to consider mandatory verification for access to social media platforms as "*an indispensable and appropriate measure in view of the risks involved*". This signals Italy's ambition for stricter enforcement of Article 28 of the DSA. • **EU-wide Digital Age of Majority Proposal**: Italy has signed the proposal led by France, Greece and Spain to establish an EU-wide digital age of majority, which would restrict minors' access to social media. • **AGCOM and Garante Joint Initiative**: On 12 April 2023, the AGCOM and Garante have set up an ongoing joint initiative to create a code of conduct to ensure digital platforms implement effective age verification.

AGCOM Standards – Key considerations

- **Double anonymity**: Ensure that the content provider cannot identify the user, and the age verification provider does not know which service the user is trying to access.
- **Technology neutrality:** Regulated services have flexibility in the choice of method, provided they comply with the established principles. Self-declaration is considered insufficient.
- **Separation of duties**: The entity verifying age must be legally and technically independent from the content provider.
- **Session-based verification**: The age assurance process must take place at each session of service use, ends (expiring automatically after 45 minutes of inactivity).
- **Data protection and proportionality**: AVS must comply with all GDPR requirements, especially the principle of minimisation and data protection by design and by default.
- **Accuracy and reliability**: AVS must be effective in containing age determination errors, both in test environments and real operating conditions. Performance should be consistent over time.
- **Robustness**: Measures to prevent cyberattacks and circumvention must be implemented.
- **Non-discrimination and accessibility**: Methods must not discriminate against certain users and must be easy to use for all users regardless of characteristics.
- **Complaints handling**: Service providers must offer at least one channel for complaints handling.
- **Non-compliant methods (deemed overly privacy-intrusive)**: Systems based on the direct collection of IDs by pornographic sites; age estimation based on users' web browsing history; use of biometric data to identify or authenticate persons (e.g., through photo-ID matching).

Netherlands

Key age assurance regulations and initiatives

Summary

The Netherlands employs a sectoral approach to online age verification, linking requirements to existing legal age limits for specific services. The EU AVMSD is implemented through an amendment to the Media Act 2008, which is enforced by the Commissariaat voor the Media (CvdM), the Dutch media authority. Discussions and regulatory initiatives to expand requirements are underway, particularly concerning the implementation of the revised European Consumer Directive (CCDII) for Buy Now Pay Later (BNPL) service providers.

Regulatory developments

Current Regulations and Guidance	• **Media Act 2008 (Mediawet):** The EU AVMSD is implemented in the Netherlands through an amendment to the Media Act (Mediawet), mandating audiovisual platforms to use technical measures for age verification, without specifying exact procedures. Video Sharing Platforms, however, are not subject to a legal age limit in the Netherlands. Without a legal age limit, online age verification cannot be prescribed in legislation, nor can the requirements for this be set out. • **GDPR**: The age of consent for personal data processing is set at 16 under national law, requiring parental consent for younger children.
Enforcement	• The **CvdM** (the Dutch media authority) is responsible for enforcing the Media Act and can impose fines for non-compliance up to €225,000 per violation. • Once in force, the **AFM** (the Dutch financial authority) will be responsible for supervision and enforcement of the Dutch implementation of the CCDII.
Emerging Regulations and Initiatives	• **Guidelines for healthy and responsible screen and social media use**: On 17 June 2025, the Dutch government released new official guidelines, aimed at parents and educators, for healthy and responsible screen and social media use among children. The key recommendation is for parents to delay children's access to social media until the age of 15. • **Revised European Consumer Directive (CCDII) Implementation into Dutch law**: Will introduce age verification requirements for BNPL providers, prohibiting providing credit to minors. • **Considerati report: 'Framework for Online Age Verification'**: Executed on behalf of the Dutch Ministry of the Interior in October 2023, it identifies the requirements for robust, private, secure, inclusive, and transparent online age verification systems and explores the considerations for selecting the most suitable verification method.

Key considerations

- **Risk-based approach**: The government adopts a risk-based approach based on the risk levels detailed in ISO/IEC DIS 27566-1 standards (still in draft).
- **Proportionality**: the use of the age verification systems must always be weighed against the risks to the protection of personal data and users' rights.
- **Non-compliant methods**: Self-declaration, system-wide solutions, and behavioural analysis or account metadata are not considered suitable substitutes for robust verification in legally regulated contexts. The processing of biometric data is banned.
- The **Considerati report** considers age verification through **direct identification** (e.g., using official identity documents) or **derived identification** (e.g., using a trusted third party) as best suited for regulated services. Importantly, using direct identification requires a legal obligation to verify age.
- **VSPs (including pornographic services):** Currently not subject to an explicit statutory age limit under Dutch law. Without a legal age limit, online age verification cannot be prescribed in legislation.
- **CCDII**: BNPL providers will have to verify the consumer's date of birth against reliable sources prior to the conclusion of a credit agreement.

Spain

Key age assurance regulations and initiatives

Summary

Spain is actively developing a regulatory framework for age assurance, focusing on protecting minors online while upholding data protection principles. Key legislation includes Ley 13/2022 (audiovisual services), which represents Spain's transposition of the AVMSD, and the draft Organic Law for the protection of minors on the internet, aligning with eIDAS 2 and the European Digital Identity Wallet (EUDI Wallet). The Spanish Data Protection Agency (AEPD) has also provided age assurance guidance through the Decalogue of principles for age verification and the protection of minors from inappropriate content.

Regulatory developments

Current Regulations and Guidance	• **General Audiovisual Communication Law (Law 13/2022)**: Mandates age verification for audiovisual media service providers, including pornographic content, to restrict minor access (Article 89). • **AEPD's Decalogue of principles:** Provides non-binding principles for age verification, emphasising proportionality and data protection. • **State Pact for the protection of minors online (2023):** Non-binding agreement promoted by the government, AEPD, and the CNMC. It gathers measures agreed with public and private stakeholders, including age verification through non-intrusive systems that respect users' rights. • **GDPR:** The age of consent for personal data processing is set at 14 under national law, requiring parental consent for younger children.
Enforcement	• The **Comisión Nacional de los Mercados y la Competencia (CNMC)** is responsible for enforcing Law 13/2022 and may impose penalties up to €1.5 million or 3% of annual income on audiovisual services in Spain.
Emerging Regulations and Initiatives	• **Draft Organic Law for the protection of minors on the internet**: This law would reinforce age verification obligations under Law 13/2022, requiring age verification systems aligned with the technical specifications of the EUDI Wallet. The draft, approved by the Government on 4 June 2024, is currently being processed under the urgent procedure before the Justice Committee. • **EU-wide Digital Age of Majority Proposal**: On 16 May 2025, France, Greece, and Spain put forward a proposal to strengthen age verification duties and introduce a pan-European digital age of majority to access social media. • **June 2025 joint letter:** Spain is among the eleven signatories of the joint letter urged the Commission to consider mandatory verification for access to social media platforms as "*an indispensable and appropriate measure in view of the risks involved*". This signals Spain's ambition for stricter enforcement of Article 28 of the DSA. • **EU white label age verification app:** Spain was one of five countries chosen to beta test the EU white label age verification app, leveraging Spain's experience with Cartera Digital Beta, a national age verification solution fully aligned with eIDAS2.

AEPD's Decalogue and Draft Organic Law – Key considerations

AEPD's Decalogue of principles

- **Data protection and privacy**: Privacy-preserving measures are encouraged as additional guarantees to comply with data protection regulation.
- **Anonymity:** Age verification systems must guarantee that identification is impossible and access to inappropriate content must be anonymous for Internet service providers and third parties. Processing biometric or browsing data is considered inappropriate.
- **Non-intrusiveness:** The obligation to prove the condition of the person "authorised to access" is limited only to inappropriate content. It should not unduly limit users' rights.
- **Accuracy and auditability:** Age verification must be carried out accurately and be auditable.
- **Non-discrimination:** Age verification systems should not discriminate among diverse users. Users must also be informed about how the age assurance process works and their rights.

The Draft Organic Law for the protection of minors online

- Requires age verification systems that guarantee levels of **security** and **privacy –** particularly regarding data minimisation, purpose limitation, and data protection by design **–** that are at least equivalent to those established for the **EUDI Wallet**. The required alignment with the EUDI Wallet may also promote EU-level **interoperability**.

Section 4

Terminology and Deloitte contacts

04

Terminology

Please note that for many of these terms there is no generally accepted definition, and the interpretation and application of these terms may differ by jurisdiction.

- **Age assurance (AA):** Umbrella term used to describe methods and technologies used to estimate or verify a person's age or age range in online environments, encompassing a variety of approaches.
- **Age verification (AV):** Any method used to determine users' age to a high degree of certainty, typically by verifying data against an identity document or verified information held by a third-party provider such as credit card data.
- **Age estimation (AE):** Any method designed to estimate the age, or age-range, of a user, often by algorithmic means. These include image-based estimation and other biometric approaches (e.g. voice analysis) or analysing a person's online activity across sites. Age estimation approaches could be considered less privacy-intrusive compared to using hard identifiers.
- **Age of consent for data processing:** Age from which parental consent is not needed to process children's data online. In EU Member States, this varies between 13 and 16.
- **Age assurance via open banking:** Works by accessing the information a bank has on record regarding a user's age, with the user's consent. The system confirms whether the user is over 18 to a third party without disclosing their date of birth or other personal data.
- **Accessibility:** Age assurance should be easy to use for all users, including by children of different ages and with different needs.
- **Accuracy:** Refers to the degree to which an age assurance method can correctly determine the age of a user. An accurate methods is characterised by high confidence in determining whether a user meets the age threshold and minimising instances of false positives/negatives.
- **Age of digital majority:** As referred to in an xEU-wide proposal put forward by France, Greece and Spain, this term refers to the age below which minors would need parental consent to access social media.
- **Anonymity:** The age is verified with no personal data or identity disclosure.
- **Challenge age:** Requiring a user who is estimated as being under a given challenge age to undergo a second age assurance step (e.g. using an age verification method) to confirm they are above the challenge age.
- **Complaints handling:** In this context, providing users with the opportunity to challenge an age assurance decision.
- **Credit card checks:** Works by asking a user to input their credit card details, after which a payment processor sends a request to check the card is valid by the issuing bank. Approval by the issuing bank can be taken as evidence that the user is over 18, as only adults can obtain a credit card in the UK.
- **Data Minimisation:** A key principle in data protection law that requires organisations to only collect and process the minimum amount of personal data necessary for a specific purpose. In age assurance, this principle supports the use of privacy-preserving methods that confirm a user meets an age threshold without revealing unnecessary personal information (e.g. using selective disclosure or zero-knowledge proofs).
- **Digital identity services:** A digital identity is a digital representation of a person's identity information, which enables them to prove who they are during interactions and transactions online and in person. Once their identity or an attribute of their identity has been verified and stored in the wallet, a user may choose to share individual attributes, such as their age, or their status as an adult, with a third party.
- **Double anonymity:** Age verification systems where the content provider cannot identify the user, and the age verification system provider does not know which service the user is trying to access.
- **Email-based age estimation:** Solutions that estimate the age of a user by analysing the other online services where that user's provided email address has been used.
- **Facial age estimation:** Works by analysing the features of a user's face to estimate their age.
- **Fairness**: Refers to the extent to which an age assurance method avoids or minimises bias and discriminatory outcomes. For example, it may mean ensuring that any method relying on artificial intelligence or machine learning has been tested and trained on data sets which reflect the diversity in the target population, and the method has been evaluated against the outcome / error parity, with results indicating that it does not produce significant bias or discriminatory outcomes.
- **Interoperability:** The ability for technological systems to communicate with each other using common and standardised formats. In this context, it refers to users being able to reuse their verified age status across services without repeating verification.
- **Liveness detection**: Anti-circumvention measure used to ensure that the face being analysed during an age assurance method is not a photograph, video, or any other form of spoofed representation used to trick the system into making inaccurate age estimates.

Terminology

Please note that for many of these terms there is no generally accepted definition, and the interpretation and application of these terms may differ by jurisdiction.

- **Mobile-network operator checks:** UK mobile network operators (MNOs) employ a system where content restriction filter (CRF) are automatically applied to SIM cards, preventing access to age-restricted websites for minors. Users can remove this filter by verifying they are over 18. The MNOs can share the status of the CRF (removed or not) with third parties as a confirmation of the user's age.
- **Non-discrimination**: A given age assurance method avoids discriminating against users. The chosen method is appropriate and available for all, regardless of disability, language, ethnic, gender, religious and minority backgrounds (see also: *Fairness*).
- **Non-Intrusiveness:** A given age assurance avoids intruding on a on users' rights. Providers may need to assess the impact that the chosen method will have on recipients' rights and freedoms, including their right to privacy, data protection and freedom of expression.
- **Photo-ID matching:** Works by capturing relevant information from an uploaded photo-ID document and comparing it to an image of the user at the point of ID upload to verify that they are the same person.
- **Portability:** Refers to the user having control over their verified age status and being able to share it across services or identity providers (e.g. a user downloading their age verification credential from one provider and share it with another service or uploading it to another wallet).
- **Privacy-preserving approach:** Approach that emphasises compliance with data protection principles (e.g. data minimisation and purpose limitation) and prioritises non-intrusive age assurance methods.
- **Profiling:** Any form of automated processing of information that is used to evaluate or predict someone's behaviour or characteristics. Profiling can be used for age assurance, e.g., through monitoring a user's vocabulary and interests to identify potentially under-age users. Ethical and legal considerations arise from profiling (particularly under the GDPR) requiring that it is transparent, proportionate, and subject to appropriate safeguards to prevent misuse.
- **Proportionality**: In this context, proportionality refers to striking a balance between the means used to achieve an intended objective and its impact on the limitation of the rights of persons. It requires considering whether, among fit for purpose measures, the chosen measure is the least intrusive option available, interfering the least with user rights, including those of children.
- **Reliability:** The degree to which the age output from an age assurance method is reproducible and derived from trustworthy evidence. For example, a self-signed proof of age would not be considered reliable.
- **Risk-based approach:** Adopting age assurance methods that are appropriate and proportionate to the risks assessed on a service and the potential harm to users.
- **Robustness:** Refers to the degree to which an age assurance method can correctly determine the age of a user in actual deployment contexts. Robustness relates to how easy it is to circumvent a given method, as well as the method's ability ensure the integrity of the age data.
- **Selective disclosure:** A feature of tokens, credentials and attestations that allows data subjects to share only the information they want with specific parties on a case-by-case basis.
- **Self-declaration:** Methods that rely on users to supply their age or age range, without requiring evidence to prove the declaration, e.g. clicking a button to confirm being 18+. This approach in isolation is widely considered an insufficient age assurance method.
- **Separation of duties:** The entity verifying age is legally and technically independent from the content provider.
- **Session-based verification:** Age assurance is required at each session of use of a regulated service.
- **Technology-neutral approach:** Regulated services have flexibility in the technological solution they may use to assure users' age.
- **Waterfall technique:** The combination of multiple age assurance approaches (e.g. age assurance combined with secondary age verification) to provide a higher level of confidence than a single approach used in isolation.
- **Zero-Knowledge Proof (ZNP):** A method in which one party can demonstrate to another party that something is true, without revealing any further information beyond the fact that it is true.

Authors

EMEA Centre for Regulatory Strategy

Suchitra Nair
Partner
snair@deloitte.co.uk

Robert MacDougall
Director
rmacdougall@deloitte.co.uk

Nick Evans
Senior Manager
nickaevans@deloitte.co.uk

Giulia De Bernardi
Senior Analyst
giuliadebernardi@deloitte.co.uk

The EMEA Centre for Regulatory Strategy is a source of critical insight and advice, designed to assist clients to anticipate change and respond with confidence to the strategic and aggregate impact of regulation.

France

Sidy Diop
Partner
sidiop@deloitte.fr

Anael Bourrous
Manager
abourrous@deloitte.fr

Belgium

Matthias Vierstraete
Partner
mvierstraete@deloitte.com

Willem-Jan Cosemans
Director
wcosemans@deloitte.com

Germany

Martin Ritter
Partner
maritter@deloitte.de

Maria Chernyshov
Senior Manager
machernyshov@deloitte.de

Italy

Ida Palombella
Partner
ipalombella@deloitte.it

Pietro Boccaccini
Director
pboccaccini@deloitte.it

Ireland

Nicola Flannery
Partner
niflannery@deloitte.ie

Lorena D'Alberton
Senior Manager
ldalberton@deloitte.ie

Netherlands

Simone Pelkmans
Partner
spelkmans@deloitte.nl

Tom Plusjé
Senior Consultant
tplusje@deloitte.nl

Spain

Rodrigo Gonzalez Ruiz
Partner
rgonzalezruiz@deloitte.es

Mireia Colomo Cardona
Lawyer
mcolomocardona@deloitte.es

United Kingdom

Nick Seeber
Partner
nseeber@deloitte.co.uk

Joey Conway
Partner
jconway@deloitte.co.uk

Laurie Gilchrist
Director
lgilchrist@deloitte.co.uk

Deloitte.