Age Assurance as a spectrum

A risk-based approach from a European perspective

5RIGHTS FOUNDATION

About 5Rights Foundation

5Rights develops new policy, creates innovative frameworks, develops technical standards, publishes research, challenges received narratives and ensures that children's rights and needs are recognised and prioritised in the digital world.

While 5Rights works exclusively on behalf of and with children and young people under 18, our solutions and strategies are relevant to many other communities. Our focus is on implementable change and our work is cited and used widely around the world. We work with governments, inter-governmental institutions, professional associations, academics, businesses, and children, so that digital products and services can impact positively on the lived experiences of young people.

FEBRUARY 2026

Contents

Foreword

Age is a hot topic in today's digital debates, as societies grapple with the fact that, in little more than a decade, tech has fundamentally reshaped childhood and children, modulating their relationships, their habits, their interests, their views – what they do, what they feel, what – and how – they think.

Recognising children and catering for them in the digital environment is a moral and legal imperative. It is only by checking age that we can shield young minds from practices, spaces, and content unsuitable for their stage of development. Acknowledging age also opens the door to a rich ecosystem of child-centric and inter-generational systems and spaces where children and communities as a whole can thrive.

In an era when tech companies often know more about their 'users' than individuals do themselves, discussing recognition of such a basic parameter as age may seem incongruous. Yet resistance to formal 'age assurance' has been fierce. For many companies, it spells the end of a very lucrative widespread case of selective amnesia; recognising children and implementing their rights will certainly curb both profits and power. For those who, like 5Rights, fight for individual privacy and agency, corporate age checking also carries the risk of further commercial exploitation.

Strong popular demand for protections for children, together with the adoption of new regulatory and technical standards, have however changed the equation. We are now at a point where age assurance can be done well, generate trust, and encourage the emergence of a digital services market that responds to demand and caters to children and inter-generational communities.

But this outcome is not inevitable. Tech companies are fast announcing new age policies and checks, seeking to pre-empt the implementation of the new rules. Policymakers are debating blanket bans for children – a blunt use of age assurance that would take the burden off companies for age-appropriate design, and off regulators harassed for poor enforcement action.

Age assurance is the gateway to a better digital world for children and their communities. If it is to deliver on this promise, it must done right, and it must be done not in isolation but as an enabler of age-appropriate design.

This report aims to provide a succinct framework for an effective, outcomes-focused, and rights-based implementation of age assurance in a European legal context. Building on a body of 5Rights work including expert reports, technical standards and ongoing research into the reality of corporate practices and children's experiences with age assurance technologies, it provides a practical guide to the assessment of age assurance tools and methods, together with case studies to illustrate their potential application in diverse circumstances.

Finally, the report closes with recommendations to policymakers, regulators, and industry, in whose hands the fate of childhood in the digital era rests. We urge them to treat it with the care that it deserves, and together we can look forward to the rich rewards of a digital environment that enables future generations to thrive.

LEANDA BARRINGTON-LEACH
5Rights Executive Director

In a perfect digital world for kids and teens, technology would be safe and fun to use. Everyone's personal information would be secure, so parents wouldn't have to worry about privacy. Online spaces would be full of cool, educational content that sparks creativity and encourages teamwork.

MARINA, 16, KAZAKHSTAN

Introduction

In 2021, 5Rights Foundation published *But how do they know it is a child?*,[1] which answered key questions about why and when age assurance is needed and explored age assurance methods to recognise children in the digital environment. The report called for a statutory code of practice and established 11 standards for future regulations. Although focused specifically on the United Kingdom, its findings were relevant globally.

Since then, many countries in Europe and beyond have passed regulations that refer directly to age assurance. Additionally, the Institute of Electrical and Electronics Engineers (IEEE) Standards Association adopted its *2024-2089.1 Standard for Online Age Verification*,[2] providing processes for digital services to verify or estimate the age or age range of users. However, despite these positive developments, challenges remain, as many companies still fail to account for the presence of children on their services and as a result, expose them to various risks and harms.

In this context, age assurance tools are often presented solely as a means of age-gating children. As this report demonstrates, this is a rather limited view. When implemented effectively, age assurance can protect children online by enabling age-appropriate design and providing a rights-respecting experience that meets children's needs.

Protecting minors online is a key priority for the European Union under the current mandate.[3] In 2024, European Commission President Ursula von der Leyen pledged to tackle cyberbullying, take action against addictive design, and investigate the impact of social media on mental health.[4] More recently, in her State of the Union Address delivered in September 2025, she stated that the European Union should consider introducing age-based restrictions on social media.[5] Later, she further clarified that she shared the view of many Member States that 'the time has come for a digital majority age for access to social media'.[6]

This growing interest at EU level mirrors ongoing discussions across Member States on protecting children online. National initiatives ranging from social media bans to a digital age of majority and smartphone restrictions in schools have been proposed. Among these measures, age assurance is posited as a critical, and in some cases even essential, tool. Reflecting this position, ministers from 27 countries agreed on 10 October 2025 on a joint declaration, calling for 'effective and privacy-preserving

age verification on social media and other relevant digital services that pose a significant risk to minors'.[7]

In many of these discussions, age assurance is limited to systems that verify users' ages and restrict those under 15 or 16 from accessing certain online spaces, notably social media. However, the European Commission's *Guidelines on measures to ensure a high level of privacy, safety, and security for minors online*[8] position age assurance neither as a silver bullet nor as a standalone tool, but rather as one potential mitigation measure within a child rights approach to the digital environment.

This report refocuses the debate on children's established rights, safety-by-design, and age-appropriate approaches. It provides an overview of the European Union's policy and regulatory context and the international framework of children's rights in the digital environment, demonstrating how European legislation supports a risk-based approach to age assurance.

Drawing on extensive research, recommendations, and standards, it establishes key principles applicable globally and offers practical guidance for policymakers and industry while the illustrative examples demonstrate how to adapt age assurance tools to the risks and specificities of different services, rather than relying on 'one-size-fits-all' solutions.

Finally, the report outlines concrete recommendations for European policymakers, regulators, and companies. These recommendations position age assurance tools as one component of a broader rights-based approach to creating safe and age-appropriate online experiences for all children.

I think [restricting certain features by age] would be good in terms of protecting people's privacy, but it should be limited so that it doesn't restrict information.

JULIA, 16, IRELAND

Definitions

For the purpose of this report, the following definitions are used:

AGE ASSURANCE

An umbrella term for both age verification and age estimation solutions. 'Assurance' refers to the varying levels of certainty that different solutions offer in establishing an age or age range.[9]

AGE VERIFICATION

A system that relies on hard (physical) identifiers and/or verified sources of identification to provide a high degree of certainty in determining a user's age. It can establish the identity of a user or be used to establish age only.[10]

AGE ESTIMATION

A process that establishes a user is likely to be of a certain age, falls within an age range, or is over or under a certain age. Age estimation methods include automated analysis of behavioural and environmental data, comparing a user's interactions with a device with patterns typical of other users in the same age group, and metrics derived from motion analysis or by testing their capacity or knowledge.[11]

AGE LIMIT

The upper limit of the age range to which a legal protection applies.[12]

CHILD

Anyone under the age of 18.

In a perfect digital world, I ensign an environment that doesn't merely prohibit children and youth as a quick fix, but a safe digital world where young people are taken into consideration. Their privacy, needs, safety and wellbeing are safeguarded through effective legislation and enforcement.

RACHEL, 20, MALTA

CHAPTER 1

Children's rights in the digital environment

All age assurance measures must be implemented in line with children's rights that are recognised in international law.

In 1989, the UN General Assembly adopted the *UN Convention on the Rights of the Child* (UNCRC),[13] which has been ratified by all EU Member States. The Convention defines a child as anyone under the age of 18 and sets out interdependent rights, including (but by no means limited to):

| ARTICLE 6 | The right to life, survival, and development

| ARTICLE 12 | The right to be heard on all matters affecting them

| ARTICLE 13 | The right to freedom of expression, including freedom to seek, receive, and impart information and ideas of all kinds

| ARTICLE 14 | The right to freedom of thought

| ARTICLE 16 | The right to privacy

| ARTICLE 17 | The right to access information from diverse sources and protection from injurious material

| ARTICLE 19 | Protection from all forms of physical or mental violence, injury, abuse, maltreatment, or exploitation

| ARTICLE 27 | The right to an adequate standard of living

| ARTICLE 28 | The right to education

| ARTICLE 31 | The right to leisure, to engage in play and recreational activities appropriate to the age of the child

| ARTICLE 32 | Protection from economic exploitation

| ARTICLE 34 | Protection from all forms of sexual exploitation and abuse

Underpinning all these rights, Article 3 of the Convention establishes that the **best interests of the child** must be a primary consideration in all actions concerning children. This principle aims to ensure the full and effective enjoyment of all the rights and the holistic development of a child,[14] and has three distinct applications:

- **A substantive right**
  The right of the child to have their best interest taken as a primary consideration when different stakes are being considered.

- **An interpretative legal principle**
  When a legal provision is open to more than one interpretation, the one that most effectively serves the child's best interests should be chosen.

- **A rule of procedure**
  Decision-making must include an evaluation of the possible impact on the child or children concerned and a justification for the choice made.[15] This justification must draw on robust evidence examined by qualified professionals and must take full account of children's concerns and wishes.[16]

The best interests of the child have implications for all implementation measures taken by governments and all decisions made by companies providing services likely to impact children. It must be central to the resolution of any conflict or tensions between the various rights outlined in the Convention. As the Digital Futures for Children centre notes, 'determination of those best interests makes it possible to identify which right(s) are to be given precedence when they are not automatically aligned (as when, for example, freedom and agency may jeopardize safety, or privacy concerns may put health at risk)'.[17] In these cases, the age and maturity of the child must be taken into consideration.

The principle of evolving capacities recognises the gradual acquisition of competencies, understanding, and agency as children grow and develop.[18] When there is a conflict between different rights or the interests of different parties, the Convention requires a thorough contextual assessment based on the child's best interests. This assessment must consult children appropriately in line with their evolving capacity.

The General comment No.25

In 2021, the Committee on the Rights of the Child adopted its *General comment No. 25*,[19] which explicitly recognises that children's rights must be respected, protected,

and fulfilled in the digital environment. Building on *General comment No. 16*,[20] which states that all businesses must meet their responsibilities to respect children's rights, *General comment No. 25* sets out provisions relevant to age verification, safety-by-design and age-appropriate approaches, including:

- Meaningful access to digital technologies can support children to realise the full range of their civil, political, cultural, economic, and social rights (§4).
- The requirement for digital services to offer or make available services to children that are appropriate to their evolving capacities (§19-21).
- The requirement for integration of safety-by-design and privacy-by-design into digital products and services that affect children (§70, 77, 88, 116).
- The requirement not to curtail children's access to the digital environment as a whole or interfere with their opportunities for leisure or other rights (§111).
- A recommendation that robust age verification systems should be used to prevent children from acquiring access to products and services that are illegal for them to own or use (§114).

Guidelines

In addition to these international human rights frameworks, regional or international entities have also clarified the application of children's rights to the digital environment. For example, the Council of Europe adopted its *Guidelines to respect, protect and fulfil the rights of the child in the digital environment* in 2018,[21] stating that:

- Access to and use of the digital environment is important for the realisation of children's rights and fundamental freedoms, including their inclusion, education, participation, and development of family and social relationships. Where children lack access to the digital environment or where this access is limited due to poor connectivity, their ability to fully exercise their human rights may be affected (§10).
- Any protective measures should take into consideration the best interests and evolving capacities of the child and not unduly restrict the exercise of other rights (§50).
- States should require services to use effective age verification systems when products, services, or content in the digital environment are legally restricted by age, ensuring these systems follow principles of data minimisation (§56).

Similarly, *the Guidelines for Industry on Child Online Protection*[22] published by the International Telecommunications Union in 2020 further note:

- Internet access is fundamental to the realisation of children's rights (p. 3).
- Age verification processes can help vendors of age-restricted goods and services, or publishers of age-restricted material reach their appropriate audiences (p. 7).
- Technology identifying users' ages and present them with age-appropriate versions of the application they are using should be implemented. For age-sensitive content or services, age verification should be used to limit access to content or material that, either by law or policy, is intended only for users above a certain age (p. 32).
- Companies should recognise the potential for such technologies to be misused in ways that restrict children and young people's right to freedom of expression and access to information or endanger their privacy (p. 32).

More recently, in 2021, the OECD released its *Recommendation of the Council on Children in the Digital Environment*,[23] calling on States to:

- Regularly take steps necessary to prevent children from accessing services and content that could be detrimental to their health and wellbeing or undermine their rights, and continue to review and improve the efficacy of those where necessary (p. 12).
- Ensure restrictions that prevent children below certain ages from accessing a service are proportionate to risk, privacy-preserving, and enforceable, when laws or policies require age-based restrictions (p. 12).

Industry standards

Beyond international law, guidelines, and recommendations, industry standards provide valuable guidance for the implementation of age assurance measures. Several standards have emerged in recent years, with the main options being developed by the Institute of Electrical and Electronics Engineers (IEEE) and the British Standards Institution (BSI). The IEEE 2089.1 standard,[24] which has recently received a related certification scheme, provides a framework for the design, specification, evaluation, and deployment of age assurance technologies. Written with a child-rights approach and grounded in the 5Cs categorisation of risks[25] – content, contact, conduct, contract, and cross cutting - it contains five levels of assurance, each with specified requirements for accuracy, duration, and level of authentication. The standard is designed to be compatible with the BSI's Publicly Available Specification (PAS) 1296:2018.[26]

By contrast, PAS 1296:2018 is not a traditional standard that sets detailed requirements but rather provides principles against which organisations can claim conformity. Certification bodies have also developed their own 'standards' for assessment based on the aforementioned standards. For example, the Age Check Certification Scheme (ACCS) has released ACCS 1,[27] addressing testing procedures for age estimation technologies.

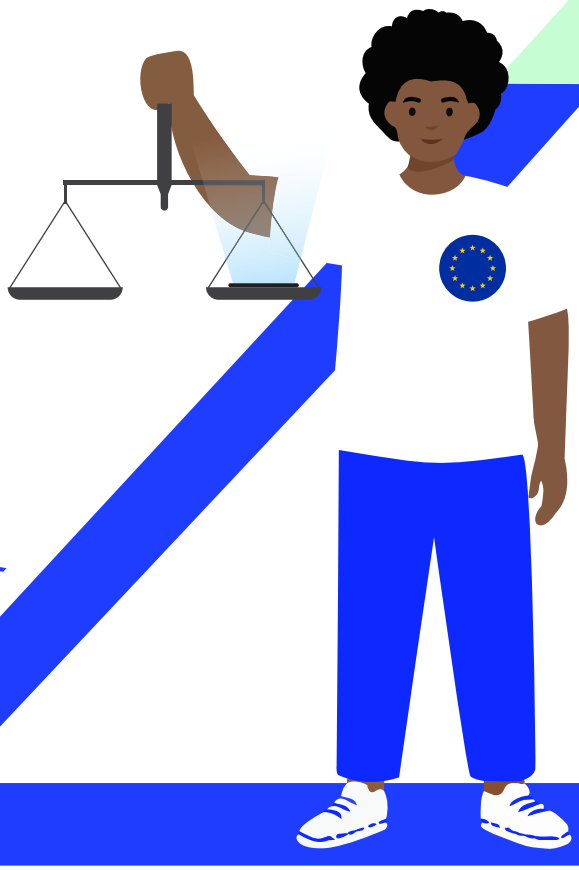
Key takeaways

Access to the online environment has been recognised as crucial for the realisation of children's rights, including their rights to education, information, play, and more. However, in certain high-risk situations, limiting children's access to parts of the online environment can be justified to prevent them from accessing content, products, services, features, or spaces that are not appropriate for their age. Age assurance is equally important for restricting some companies' access to children and prevent them from commercially exploiting them.

As established by the UNCRC and reinforced by international and regional frameworks as well as industry standards, age restrictions must be implemented in line with the best interests of the child and their evolving capacities. Misusing or abusing this ability to limit children's access would undermine their rights, freedoms, and interests.

Age assurance tools have a role to play, not simply to restrict access, but as part of a broader rights-based approach that ensures meaningful access to the digital environment for children. This requires redesigning digital products and services to be age-appropriate, safe, and private by design. Age-appropriate design is substantiated in depth by standards such as IEEE 2089.[28]

CHAPTER



Policy & regulatory context in the European Union

Building on these international commitments, the European Union has established its own frameworks and laws to protect and empower children online.

The *European Charter of Fundamental Rights* enshrined the rights of the child in Article 24 in 2000.[29]

In 2021, the *EU Strategy on the Rights of the Child* called on Information and Communication Technology (ICT) companies to ensure that 'children's rights are included in digital products and services by design and by default'.[30] A year later, the *European Strategy for a Better Internet for Kids*[31] strongly emphasised age-appropriate digital services. Both frameworks recognise the lack of effective age verification systems as contributing to children's increased exposure to harmful content.[32]

To support the effective and proportionate implementation of age assurance, the *Better Internet for Kids* initiative developed a self-assessment tool[33] based on the report *Mapping age assurance typologies and requirements*.[34]

In 2023, the *European Declaration on Digital Rights and Principles for the Digital Decade* further committed the Union to protecting and empowering children in an age-appropriate and safe digital environment.[35]

Several European laws further shape the online environment for children.[36] The General Data Protection Regulation (GDPR) upholds the right to the protection of personal data, the Audiovisual Media Services Directive (AVMSD) regulates content, notably on video sharing platforms and the Digital Services Act (DSA) sets obligations for online intermediaries and platforms.

The General Data Protection Regulation

Under the *General Data Protection Regulation*,[37] adopted in 2016, all data processing must be based on legal grounds set out in Article 6. When consent serves as the legal basis for processing (GDPR, Art. 6(1)(a)) the personal data of a child under 16, parental consent is required for services directly offered to a child (GDPR, Art. 8(1)). Member States may set a lower age threshold, provided it is not below 13 (GDPR, Art. 8(1)).

Although the GDPR does not explicitly require age verification, providers may need to determine whether users have reached the minimum age for giving consent, or whether a higher level of personal data protection is required because the data subject is a child.

Therefore, some Data Protection Authorities have provided national guidelines on age assurance.[38] For instance, in their *Recommendations on the Digital Rights of Children,*[39] the French Commission National de l'Informatique et des Libertés (National Commission on Informatics and Liberty - CNIL) recognises that age-checking systems must be in place for certain apps and sites. Similarly, the Irish Coimisinéir Cosanta Sonraí's *Fundamentals for a Child-Oriented Approach to Data Processing*[40] states that online service providers must identify their users and ensure tailored experiences for children. Additionally, the Fundamentals emphasise that services cannot bypass their obligations by denying children access to their entire platforms.

The GDPR also applies to the processing of personal data within age assurance systems. In February 2025, the European Data Protection Board provided further clarity on the matter by adopting a *Statement on Age Assurance* that establishes ten high-level principles:[41]

1. **Full and effective enjoyment of rights and freedoms:** Respect all fundamental rights, with the best interests of the child as a primary consideration.

2. **Risk-based assessment:** Implement age assurance in a risk-based and proportionate manner compatible with rights and freedoms.

3. **Prevention of data protection risks:** Ensure age assurance does not create any unnecessary data protection risks.

4. **Purpose limitation and data minimisation:** Process only age-related attributes that are strictly necessary for their specified, explicit, and legitimate purpose.

5. **Effectiveness:** Demonstrably achieve a level of effectiveness adequate to the purpose.

6. **Lawfulness, fairness, and transparency:** Ensure all personal data processing is lawful, fair, and transparent to users.

7. **Automated decision-making:** Comply with the GDPR and provide suitable safeguards for rights, freedoms, and legitimate interests.

8. **Data Protection by design and by default:** Design, implement, and evaluate age assurance methods using most privacy-preserving approaches and technologies.

9. **Security:** Implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

10. **Accountability:** Establish governance methods to demonstrate compliance with legal requirements.

The Audiovisual Media Services Directive

Under the *Audiovisual Media Services Directive,*[42] reviewed in 2018, video-sharing platforms (VSPs) must implement appropriate measures to protect minors from content that could impair their physical, mental, or moral development (AMSD, Art. 28b 3(f)). These measures, which explicitly include age verification tools, must be proportionate to the potential harms. The most harmful content, such as excessively gratuitous violence and pornography, is subject to the strictest access control measures (AVMSD, Art. 6a and 28b 3(f)).

The AVMSD also enshrines the country-of-origin principle, meaning VSPs fall under the jurisdiction of the regulatory authority in the country where they are established. Since most major online platforms have established their EU headquarters in Dublin, Irish regulation plays a particularly important role. To implement article 28 of the AVMSD, the Irish regulator Coimisiún na Meán adopted the *Online Safety Code* in 2024.[43] The Code requires services that do not exclude adult-only video content to implement effective age assurance measures, with the appropriateness of these measures depending on the size and nature of the platform (Online Safety Code, p. 3). The Code also clarifies that self-declaration of age is not considered sufficient.

The Digital Services Act

Under the *Digital Services Act,*[44] online platforms accessible to minors must ensure a high level of privacy, safety, and security for children (DSA, Art. 28.1) and shall not present advertisements based on profiling of minors (DSA, Art 28.2).

The European Commission's *Guidelines on measures to ensure a high level of privacy, safety, and security for minors online,*[45] published in July 2025, further clarify which measures are considered appropriate and proportionate under Article 28.1.

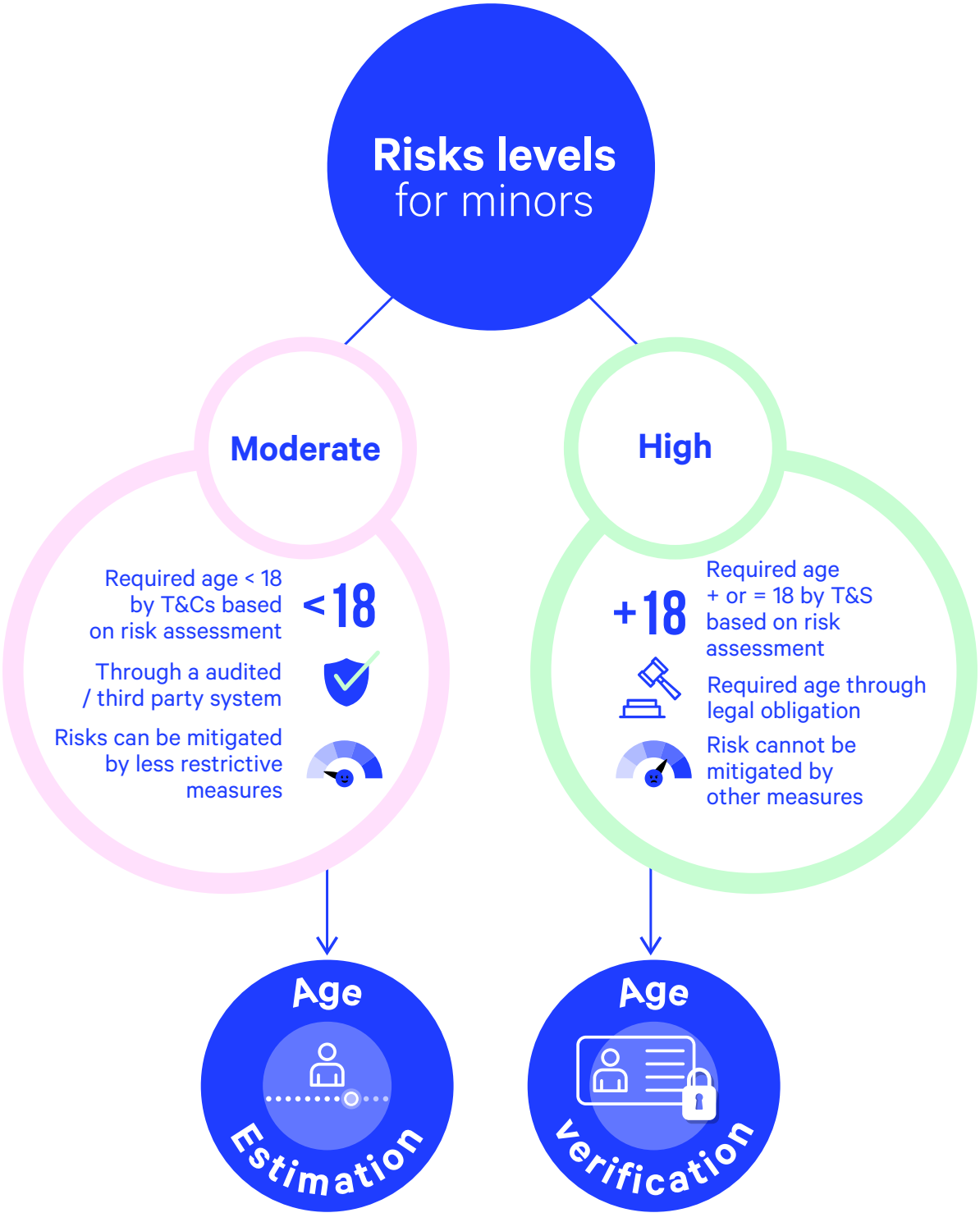
These include age assurance tools as one measure for restricting access based on age (§25). They can serve a dual purpose: preventing adults from accessing platforms designed for minors and preventing children from accessing age-inappropriate content and features (§25-26).

The guidelines establish a three-step process for implementing age assurance:

1. **Determine whether access restrictions are necessary:** Providers must conduct an assessment to determine whether such measures are appropriate and proportionate to the identified risks.

2. **Select appropriate age assurance methods based on context:** The choice between age verification and age estimation depends on the level of risk and the specific circumstances. **Age verification** is likely to be used when the service entails high risks to minors, Terms & Conditions (T&Cs) require users to be 18 or over due to identified risks, risks cannot be mitigated by other less intrusive measures, Union or national law prescribes a minimum age to access certain products or services (e.g., for gambling). **Age estimation** is likely to be used when T&Cs require users to be above a required minimum age lower than 18, based on the provider's risk assessment, the service entails medium risks to minors that can be mitigated by less restrictive measures, the method is provided by an independent third party or through systems appropriately and independently audited for security and data protection compliance.

Choice between age verification and age estimation



3. **Assess the appropriateness and proportionality of the selected age assurance methods.** Age assurance methods must meet the following criteria:
   Accurate – accuracy in determining users' age must be regularly verified using publicly available metrics.
   Reliable – methods must function effectively in real-world circumstances.
   Robust – methods must not be easily circumvented by minors.
   Non-intrusive – methods must not severely impact other rights and freedoms.
   Non-discriminatory – methods must be appropriate and available for all users.

The guidelines also clarify that self-declaration is not considered an appropriate age assurance method because it is too easily circumvented (§47b, 52).

However, the guidelines do not specify what constitutes a 'high risk' in comparison to a 'medium risk'. The risk review refers to the 5Cs typology of online risks to children[46] – content, contact, conduct, contract, and crosscutting – and requires platforms to indicate the level of risk for minors (low, medium, or high) based on clear criteria (§18b).

While the guidelines explicitly recognise the potential of age assurance tools to underpin age-appropriate design of services (§27, §48), they do not specify when this would be deemed appropriate and proportionate, nor the specific type(s) of age assurance that would be suitable for this purpose.

Beyond these general requirements, Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) face additional measures. They must identify and assess systemic risks to children's rights and protection, as well as serious negative consequences for a person's physical and mental wellbeing (DSA, Art 34). Based on this assessment, they must implement reasonable, proportionate, and effective mitigation measures. These may include adapting the design, features, or functioning of their services, as well as deploying targeted measures to protect children's rights. These measures may include age verification tools, amongst others (DSA, Art 35).

In practice, this means that if a platform offers services that do not meet adequate standards of privacy, safety, and security for children, the provider should prevent children from accessing it through appropriate, proportionate, and privacy-respecting age assurance measures.

To ensure compliance, Digital Services Coordinators have the power to order remedies for infringements and, when appropriate, impose fines to non-compliant providers.

In the most serious cases, they can request that the competent judicial authority order a temporary restriction of access to the service (DSA, Art. 51).

Key takeaways

The European Union has established a legislative framework, through the DSA, GDPR, and the AVMSD, that supports a risk-based approach to age assurance, with clearer obligations for online platforms and video-sharing platforms. The DSA places the onus on providers to ensure their services meet high standards of privacy, safety, and security. If a service poses high risks for children, it should not be accessible to them. Moreover, age assurance tools should be used to recognise children on the platform, and prevent their commercial exploitation, particularly through the prohibition of personalised advertising based on profiling of their personal data. However, some sectors and industries, such as gaming and smaller businesses, fall outside the scope of the DSA, creating potential gaps in protection.

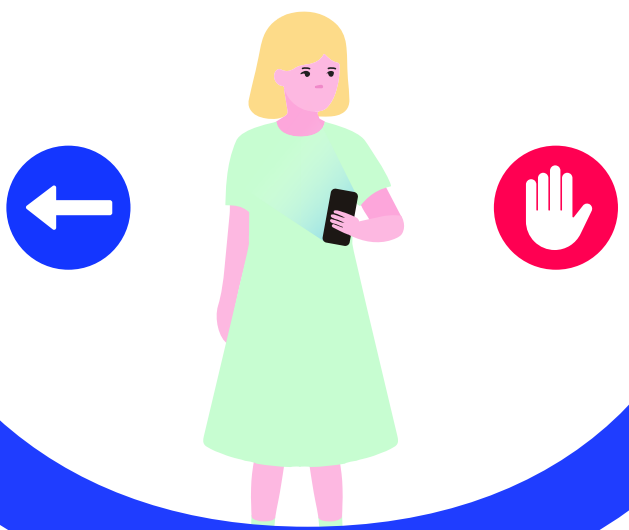
The DSA *Guidelines on measures to ensure a high level of privacy, safety, and security for minors online* propose a three-step process to assess whether and when to implement age assurance and how to choose the appropriate and proportionate methods. The Guidelines also clarify that age verification can be used when national law establishes a minimum age to access certain online products or services, including 'specifically defined categories of online social media services'.[47] However, fragmented national approaches risk creating uneven protection across the European Union, ultimately undermining consistent safeguards for all children in Europe.

It is also worth noting that the ongoing discussion about a minimum age to access social media mostly refers to age assurance as a measure for restricting access of children, reflecting a limited perspective. Age assurance measures should be understood more broadly as part of a comprehensive approach that enables age-appropriate experiences and protects children within the digital environment. Rather than simply gatekeeping access, age assurance should be a gateway towards online experiences tailored to children's developmental needs and evolving capacities.

I think the combination of age check and content blurred with warning that it may be harmful to mental health or age-inappropriate would be really helpful, more than just age check alone.

FLORENCE, 19

CHAPTER



Principles for implementing age assurance

The following guiding principles should underpin the use of age assurance by digital services providers, ensuring its implementation respects children's rights and aligns with the European regulatory and policy framework. Overall, any age assurance method must be lawful and rights-respecting, not only for children but also other users, with the best interests of the child remaining a primary consideration.[48] This means considering the full spectrum of rights, including the rights to privacy, freedom of expression, access to information, and non-discrimination as well as children's evolving capacities.

Consulting with children is central to this rights-respecting approach and in line with their right to be heard and to participate. In consultations undertaken by 5Rights Foundation, children clearly state that age checks are important to them, but that they need to 'trust the checking'. Their concerns and preferences reveal crucial considerations for implementation.

Children are particularly concerned about who conducts the age checks. If platforms themselves perform age checks, children fear it could lead to increased surveillance and a lack of respect for their data privacy.[49] They also find capacity testing and biometrics off-putting and, despite being generally comfortable with sharing images of their faces, are concerned about the use of their data and prefer to place their trust in third-party token mechanisms.[50]

Beyond concerns about implementation, children emphasise that they will only respect age assurance if they feel it is legitimate. Some find it useful for a company to know a user's specific age if it ensures safe and age-appropriate access or enforces limits on features or content unsuitable for younger children.

However, regardless of the purpose, they consistently ask for transparency and privacy safeguards.[51] Children also stress the importance of understanding why age checking is necessary and value clear communication, such as warnings about the risk of harmful content or harm to their mental health.

Risk-based and proportionate

Age assurance measures should be risk-based and proportionate to the risks arising from the product or service.[52] This means implementing age assurance only when necessary, on products or (parts of) services that children are likely to access. The type of age assurance used will depend on its purpose and the level of risk children would be exposed to.

Providers of products or services that are likely to be accessed by children can follow two primary approaches:

1. **Re-design their services or products to become safe, secure, and private for all users, including children:** Where possible, services and products should be designed to be suitable for all users, including children, eliminating the need for age assurance. In other words, the most suitable solution implies designing out any harmful practices, features, and functionalities and proactively prioritising safety and privacy by design and default for everyone.

2. **Implement proportionate age assurance measures based on risk assessment:** Age assurance should always be understood as part of a broader age-appropriate design strategy, tailoring services for their users as they grow. This can include age-gating access to certain features, functionalities, or content categories, or even to services as a whole (e.g., for younger children). In all cases, the measures implemented must be necessary, proportionate to the risk, and transparent. Age-gating can never be used by companies to avoid their responsibilities to make their services age-appropriate for all children who access them in practice, including older children when restrictions for younger children are in place.

The effectiveness, proportionality, and robustness of age assurance measures must be weighed against their potential impact. Providers must assess age assurance tools to consider the positive and negative effects on children's rights, ensuring rights are not disproportionately or unduly restricted and positive impacts are maximised. This assessment must account for the full spectrum of rights, including children's right to participate, to privacy, to protection of personal data, to play, and to information.

In practice, this requires conducting a Child Rights Impact Assessment (CRIA)[53] to identify and evaluate the risks that the service poses to children.[54] A CRIA also provides an opportunity to consult with children and other relevant stakeholders, including parents and children's rights experts.[55]

Privacy-preserving and secure

Age assurance measures must be secure and must align with children's privacy rights and data protection law. Additionally, they must abide by the principles of data minimisation and purpose limitation and remain robust over time.[56]

To respect data minimisation, providers should collect only the minimum amount of information necessary to establish age or the age range[57] and this data can never be used for any other purpose. Moreover, age assurance should not entitle providers to store personal data beyond the user's age group information.[58] Throughout the design and implementation process, age assurance systems must embed data protection by design and by default,[59] with effective safeguards preventing unnecessary data protection risks.[60]

Beyond data minimisation, appropriate technical and organisational measures must be established to ensure a high level of security.[61] This is particularly significant considering the sensitive nature of the personal data involved in age assurance.

Some researchers[62] have focused on or mentioned practical examples demonstrating how age assurance can be implemented in a privacy-preserving way. The Spanish Agencia Española de Protección de Datos (Spanish Data Protection Agency - AEPD) published a Proof of Concept[63] and a more general Technical Note.[64] Similarly, the French Commission Nationale de l'Informatique et des Libertés (CNIL) has published research on age verification systems that enable users to access restricted websites without sharing personally identifiable data beyond age itself, using a certified third party.[65] In this context, double blind methods are of particular interest, since they do not reveal the identity of the user to the requesting party, nor the identity of the requesting party to the assurer. Standards such as IEEE 2089.1[66] and ISO/IEC 27566-1[67] provide frameworks that can guide organisations in implementing these privacy-preserving approaches effectively.

Effective

Age assurance measure must be effective in determining that a user is above a minimum age, below a maximum age, or within a specific age range. To be effective, the method used must not be easily circumventable[68] and it must be robust and reliable.[69] This also means that it should not rely on self-asserted information.[70] Different age assurance methods can – and often should – be layered and used together to ensure effectiveness as well as accessibility.

Accessible and inclusive

Age assurance methods must be convenient and easy to use for children and other users,[71] while being accessible and suitable for all children. Services must therefore account for diverse characteristics and circumstances, including different languages, abilities, races, developmental capacities, socioeconomic statuses, access to parents/carers, and more.[72] Again, in some cases, platforms may need to provide more than one age assurance method to avoid unfair exclusion.[73] Offering multiple options could also enhance user trust[74] – for instance, offering both biometric and non-biometric options accommodates users who are less comfortable with either approach.

Transparent and accountable

As noted in the children's consultation carried out in late 2025,[75] transparency is crucial for children to build trust in age assurance methods. However, it should be clarified that child-friendly age assurance does not mean making these measures gamified or invisible: children need to understand what is happening and why. Their development relies on understanding boundaries and societal norms through experience; therefore, appropriate levels of friction should be normalised when necessary.[76] This includes providing a warning about the risks of accessing age-inappropriate spaces or services, helping children make informed decisions about their online behaviour.

Providers must clearly communicate to child users which methods are being used to verify their age, what data being is collected and processed, who is collecting and for how long, whether third parties were involved, and why an age assurance method was deemed necessary and proportionate. Further, they should explain the adequacy and effectiveness of the measures, including performance metrics.[77] This information must be presented in age-appropriate formats that children can easily understand, for example using audiovisual elements or bite-sized content.[78] Critically, the process and presentation of such information must enable genuinely informed consent that is easy and feasible for the child to provide.

In terms of accountability, actors across the ecosystem must be held accountable for operating necessary and proportionate age assurance standards.

Services relying on age assurance must provide clear, timely, and accessible routes for users to challenge incorrect age determinations and seek redress.[79]

Key takeaways

Service and product providers bear the fundamental responsibility of making their services and products safe, private, and age-appropriate. The first and most effective approach is to remove the most harmful features and functionalities, ensuring the safety and privacy of all users by design.

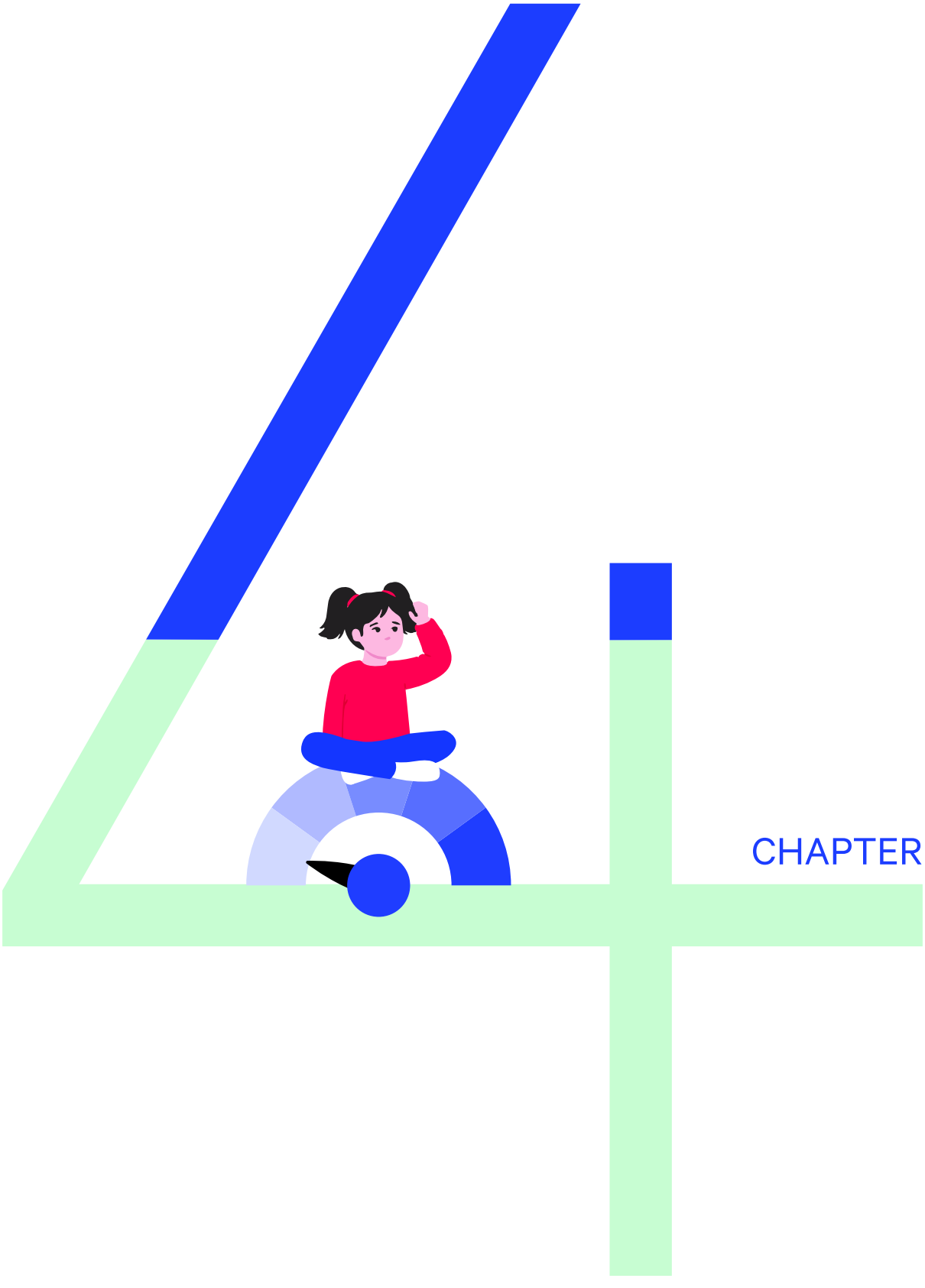
When this alone is insufficient or not feasible, age assurance can provide a set of tools to support children's right to participate and engage with digital products and services, while ensuring children have the necessary protections. The goal of age assurance is therefore to enhance children's experience and ensure they can enjoy the digital world safely, not merely restrict their access.

To achieve this goal, children must be central to the process. Including them in the design, implementation, and evaluation of age assurance measures is essential to ensure these tools are risk-based, proportionate, privacy-preserving, effective, accessible, and transparent.[80]

When implemented according to these guiding principles and informed by a comprehensive Child Rights Impact Assessment (CRIA), age assurance can achieve legitimacy and effectiveness, enabling children to enjoy safe and age-appropriate online experiences.

Companies knowing all the information that comes with sharing official documents is a little bit worrisome so I don’t know if I would be as comfortable with that.

AISLING, 17, IRELAND



CHAPTER

A risk-based spectrum of approaches

Age assurance encompasses a spectrum of approaches with varying levels of robustness and intrusiveness. This list is not exhaustive, and the range of tools is likely to expand as the industry continues to mature.

As established in the principles outlined in Chapter 3, a risk-based approach requires weighing the robustness of any age assurance method against its potential negative impacts (e.g., on privacy and inclusion) and the level of risk it aims to mitigate. This balance ensures proportionality.[81]

Determining the need for age assurance

Before selecting methods or determining where to apply age assurance, providers must first assess whether age assurance is needed at all. As stated in the report *But how do they know it's a child?*[82] there are scenarios where age assurance is unlikely to be needed:

- Products or services that are unlikely to engage with children or be of interest to them.
- Products or services specifically designed for children that already meet child-centred design criteria and a high level of privacy, safety, and security.
- Products or services specifically designed for mixed audiences that already meet child-centred design criteria and a high level of privacy, safety, and security.
- Products or services that require user identification and have already established the person's age (e.g., banking or health services).
- News media and online encyclopaedic resources that children have a right to access (UNCRC, Art. 17). These may be exempt from age limits and age assurance tools but should consider age ratings (labelling) and content warnings.

Where to apply age assurance

Once providers determine that age assurance is needed, they must decide where to apply it. Whether it is most appropriate to implement it at the device, platform, ecosystem, or feature level – or to use distinct methods at several levels – will depend heavily on contextual factors and should be assessed case-by-case.

Age assurance methods can be applied at four broad levels:

- **Device level**
  Age assurance is applied specifically on the device itself as a function of hardware or firmware. For example, a phone may determine the age of its owner and store this information locally.
- **Service level**
  Age assurance is required as a condition for accessing the service. For example, a user may be asked to verify their age to create an account on an online casino.
- **Ecosystem level**
  Age assurance operates the wider supporting environment rather than within the service or device. For example, when a user accesses a shopping website through a browser, an extension in that browser could provide age token wallets or other forms of assurance to verify a user's age.
- **Feature level**
  This a more granular approach where age assurance is applied to specific features within a service. For example, anyone may be able to create an account on a website, but certain features (e.g., gambling mechanics, algorithms that recommend harmful content) require age confirmation.

Also, different implementation approaches are possible depending on the level of risk:

- **Layered approach**
  If a service or product contains individual features that present risk, providers can use age assurance for specific features rather than the entire service.[83]
- **Service-wide approach**
  For high-risk services or those with existing legal age restrictions such as gambling or pornography, providers should implement robust verification methods across the entire service.[84] In some cases, national law explicitly requires the use of age verification systems to prevent children from being exposed to extremely violent or pornographic audiovisual content.

Regardless of the chosen level of application, the optimal approach is the one that is the least intrusive on children's rights and users' fundamental rights while meeting the required thresholds for safety and security.

Assessing robustness against risks

Once providers determine where to apply age assurance, they must select appropriate methods. In a risk-based approach, age assurance methods can be classified according to their levels of robustness, which often correlates to their level of invasiveness.

High robustness: age verification

- Third party assurance providers

  At the most robust end of the spectrum, there are approaches requiring 'hard' identifying documents such as a passport or driver's licence. While these methods provide strong verification, the revealing of unnecessary personal data creates privacy risks. They also create barriers to access, as many people lack up-to-date versions of the necessary documents, potentially excluding them from online spaces.[85] The Irish Coimisinéir Cosanta Sonraí (Data Protection Commission of Ireland – DPC) considers these methods disproportionate for verifying children's age, given that many children do not have access to the documents required.[86] Given the invasiveness of this method, it is mostly suitable when a very high level of robustness is legally required and for services restricted to users over 18 (e.g., buying alcohol).
- Hard identifiers

  The use of third-party assurance providers, such as digital identity or age tokens has the potential of providing a high level of age assurance while minimising the sharing of personal data and giving users more control. To ensure that they are sufficiently privacy preserving, these tools require the respect of privacy and data minimisation standards.

Medium robustness: varied approaches

Below age verification lie a variety of approaches, with varying levels of effectiveness depending on their specific deployment and configuration. The accuracy of some of these methods and products can differ across age groups, skin tones, phenotypes, and other characteristics, raising concerns about their fairness. This is why offering multiple approaches is often preferable to relying on a single method. Furthermore, some are more nascent than others and unproven at scale, while others may be more susceptible to adversarial inputs designed to fool the system.

Mid-spectrum approaches include:

- **Account holder confirmation**
  An adult in loco parentis is contacted to verify the age of the user. The effectiveness of this method depends on how thoroughly the adult's identity is verified and buy-in from the adult is required. Nonetheless, research from multiple countries shows that guardians may not always accurately report their child's age.[87]
- **Physical biometric methods**
  These include facial age estimation and hand measurement. While effectiveness and robustness vary significantly between tools and user groups, this approach also receives mixed feedback from users about its invasiveness. Additionally, the Artificial Intelligence models inherent to many of these methods raise concerns about data privacy, bias, and security.[88]
- **Capacity testing**
  Users complete tests designed to assign them to a likely age category. This approach is typically not very robust because it relies on normative developmental categories that do not account for the variety of child developmental trajectories. Therefore, it presents significant fairness concerns, particularly for children with cognitive disabilities.
- **Email verification**
  The history of an email address is analysed to determine the probable age of its owner. At the time of writing, little is known about the long-term sustainability and effectiveness of this approach.
- **Age inference**
  Users' behavioural data is analysed to predict a likely age or age range. This approach raises similar developmental and fairness concerns as capacity testing.

Low robustness: self-declaration

At the opposite end of the spectrum is self-declaration, the process of simply asking the user to assert that they are old enough to use a service by ticking a box or entering their date of birth. Given the ease of circumvention and the minimal protection offered, self-declaration is only suitable for low-risk products and services without features that can have a negative impact on children and their rights,[89] such as personalised features. Conversely, because processing children's data is likely to be high risk, it demands more robust assurance methods, making self-declaration wholly inadequate.[90]

Across this spectrum, age assurance systems can also combine multiple approaches, to balance robustness, accessibility, and privacy.

Key takeaways

A risk-based approach requires providers to make holistic decisions about the impact of age limits and age assurance, to ensure children's rights are respected by design.

The challenge is complex, as no single method is universally appropriate. The right choice will depend on balancing robustness against potential impacts on privacy, accessibility, and inclusion while addressing the specific risks and context of each service and product.

Crucially, the effectiveness and fairness of age assurance vary not only by method but also by implementation and user characteristics. Offering multiple methods and combining different approaches can therefore help balance robustness, accessibility, and user trust while respecting privacy and data minimisation principles.

This complexity calls for practical guidance and common standards to ensure the privacy, security, transparency, and inclusiveness of different tools.

I think a perfect digital world would include some age restrictions for social media and potentially dangerous sites, less ads that target young people insecurities, and just a safer and creative environment in general.

PIPER, 16, US

CHAPTER

Cases in applying age assurance tools in practice

The following cases explore how age assurance may factor into various points of the user journey. While these examples mimic real platforms and services in terms of functionality and scope, they are illustrative and do not represent any specific company or product. Instead, they are intentionally high-level and do not prescribe specific solutions, as the appropriate approach always depends on contextual factors, including whether age assurance is a proportionate option in the first place.

Rather than recommending specific solutions for particular platforms or functions, these examples provide practical guidance by considering diverse approaches grounded in children's rights and wellbeing.

Some examples also illustrate where age assurance should not be required. While specific tools and methods are mentioned, this does not constitute a strict recommendation to use them.

General practical guidance

In accordance with the principles outlined in the previous section and in addition to the Child Rights Impact Assessment, service providers may rely on the following practical recommendations to reduce the pitfalls of age assurance tools:

1. Embed age assurance within a comprehensive privacy by design and safety by design approach, removing harmful persuasive and habit-forming elements, implementing robust moderation in line with fair Terms of Service, and offering effective redress mechanisms to all users.

2. Provide users with clear information about where, why, and how age assurance is being implemented.

3. When a robust age assurance is legally required or needed to prevent children from accessing the most harmful content or features, use privacy-preserving third-party approaches that encourage user trust in the security of the process and ensure age tokens come from reputable sources. Do not encourage first-party collection of additional personally identifiable information (PII).

4. Respect the principle of data minimisation by prioritising anonymous age assurance approaches wherever possible. Invasive profiling methods are unlawful and can be highly biased.

5. Avoid capacity testing as the sole means of determining age as it can be highly exclusionary (e.g., for neurodivergent people or those with a different level of access to education).

6. Do not encourage additional first-party collection of biometric data beyond the scope of the existing service.

5.1 **Mobile social media app**

FriendFeed

FriendFeed is a popular social media app designed for users aged 13 and up. Users can post text, videos, and pictures, or 'like' and 'reshare' others' posts. Users can also add people as friends either by searching for their usernames or by discovering them through algorithmic recommendations. The main feed includes posts from friends, friends of friends, algorithmically suggested content, and advertisements. Users can also share their location with friends using an interactive map and engage in one-to-one direct messaging or group chats. *FriendFeed* recently introduced a feature allowing users to chat with large language model (LLM)-powered chatbots.

The company has introduced parental controls, which allow a guardian to customise settings such as profile visibility, ad personalisation, and access to specific features like the map.

FriendFeed is available as a mobile app downloaded from device app stores, which display an age rating of 12+. Users must have an app store account to download it.

The level of robustness required of age assurance in this scenario depends heavily on the app's specific features and functionalities and the level of residual risk they pose to children after any mitigations have been applied. Features and functions that often present high levels of risk to children in the context of social media include recommending adult strangers as friends, LLM chatbots, processing of children's personal data and live location sharing. When such high-risk functionalities exist on a social media service, they should be turned off by default for children.

At the device level, various options exist such as the phone requesting the user's age when creating a user profile, parental controls set up on the device, the parent indicating to their mobile service provider that the SIM card belongs to a child, or the use of specific phones designed for younger audiences.

At the ecosystem level, the app store might check for age contra-indicators between any assurance done at the device level and the app being downloaded.

At the service level, age may be self-asserted, proven through an age token, or asserted by a guardian through a consent mechanism. The method used depends on the platform in question and how it intends to process user data. For instance, a service that profiles users for advertising purposes should take reasonably robust steps to verify that the users being profiled are over the minimum age.

At the feature level, age tokens may be used to access riskier features. For instance, a social media service could allow anyone to sign up without stringent age assurance but require an age check before users can enable high-risk functionalities, view sensitive content, weaken privacy settings, or opt into more personalised recommender systems or advertisements.

5.2 **Games console and digital game download**

Royale fighter

Royale Fighter is an online multiplayer game where players compete to be the last combatant standing. Players can join games with friends registered to their console account or play with strangers. They can also add users via username or from a list of people the user has recently played with. The game enables voice communication through microphone access.

Royale Fighter is free to download on home video game consoles. However, the game includes login bonuses of an in-game currency called 'gems', which can also be purchased through microtransactions in the in-game shop.[91] Gems can be used to purchase new character tools and to buy and sell custom characters that players can create by uploading pictures.

The game has a Pan-European Game Information (PEGI) rating of 12, though the official Terms of Service require users to be 13 and up. It is downloaded from the console's integrated online store, which requires its own user account.

My house

My House is a game where players plan and decorate a house. The game is designed for offline play but offers an online mode where friends can play together, provided they know each other's passwords. Players can interact through a short-form text chat that filters out common inappropriate words and phrases. Cosmetic items are earned using the game's 'stars' currency, which has no connection to any real-world currency or value and cannot be purchased with real money.

My House is available for purchase as a physical disc or through the console's integrated online store. To download My House from the online store, players must already have a store account.

The game has a PEGI rating of 3, though the Terms & Conditions require users to be either 12 and up or have permission from a parent or guardian.

Games are an extremely diverse form of media, and each requires analysis of its own unique context. However, certain principles generally hold true in most scenarios:

- Massively multiplayer online (MMO) games will likely present a higher level of conduct and contact risk than offline or single-player games.
- Games with higher age ratings (e.g., PEGI ratings) will likely present a higher level of content risk.
- Games incorporating microtransactions will likely present a higher level of contract / commercial risk.
- Games nudging the user towards daily or habitual usage (e.g., through login bonuses) will likely present a higher level of contract / commercial risk.
- Games enabling the upload of diverse types of user-generated content (UGC) will likely present a higher level of conduct / content risk.
- Games enabling users to search for and add online strangers as friends will likely present a higher level of contact risk than those without this functionality or those requiring users to already know one another (e.g., by sharing special passwords).

Given these principles, the level of robustness for downloadable console games depends on their individual features and functionalities, particularly residual risk levels.

At the device level, pre-existing options might include requesting age at initial account setup, use of family account functions, or authentication functionality (such as passwords with multi-factor authentication and/or tokens) for accounts registered to older users in mixed-age households. Some consoles also ask which user is playing before launching said game to determine eligibility of the user.

At the service level, the storefront might offer a high default level of protection by allowing all users to browse most of the games for sale while restricting access to content such as violent screenshots or graphic descriptions until users authenticate their age. A 'safe search' option could also filter out pornographic and other age-inappropriate games for unauthenticated users.

Users may authenticate using passwords with multi-factor authentication or age tokens to access content appropriate for their PEGI age bracket, with the app store checking the age information against each game's stated PEGI rating. Importantly, PEGI is not an age assurance scheme but rather provides gamers and their families with information to make informed choices about the games they play. Therefore, it may be advisable to give guardians the option to enable PEGI-based filtering.

Additional filtering options could address high-risk features not fully captured by current PEGI standards, such as loot boxes or microtransactions that pose potential financial harm.

At the feature level, some games have granular controls, such as nudity filters, which may be integrated with age assurance in the future. Games may also have features to check a user's age and/or seek secondary consent before allowing in-game purchases.

For digital games console experiences, age assurance could complement other harm mitigations such as stringent storefront quality control, parental settings, and reports on playtime or purchases that could be made available to parental accounts. To ensure digital games console experiences are safe and transparent for children, providers could implement complementary measures to age assurance such as parental controls and labelling. Where parental controls are used, they should allow guardians to tailor their child's experience through granular options (such as disabling swear word filtering and microtransactions), while remaining clearly visible to the child. These controls must align with principles of proportionality and the best interests of the child, accounting for their evolving capacity. For instance, requiring parental verification for the download of a game rated 7+ for a 15-year-old user is not proportionate. Providers should also lean from established age rating best practices in this sector, such as PEGI.

5.3 **Pornographic website**

Adult video Hub 

Adult Video Hub is a website where users can view and upload pornographic videos. It is only accessible through a web browser, with no official app in any mobile app stores.

The service allows users to tag their videos and filter out unwanted content by blacklisting certain tags. Users can leave 'likes', comment on videos, and follow other creators. Creating an account is free but the service earns revenue through monetised 'premium' accounts (which offers additional user privileges such as higher-quality video streaming) and through targeted advertisement for other adult-only services like online casinos.

Adult Video Hub is intended only for users aged 18 and over.

Device level approaches are unlikely to be applicable in this case, as users might access a pornographic website from a variety of devices, including a shared household device used by people of varying ages.

Based on the applicable laws governing pornography and similar age-restricted products, a high level of robustness is required of age assurance tools.

At the ecosystem level, the user may have optionally installed a digital age wallet or other age assurance browser extension from a reputable third party, which is then recognised by the site.

At the service level, unauthenticated users would be expected to verify their age using some proof-of-age token.

Due to the nature of this service, **feature-level approaches** are unlikely to be applicable.

Complementary measures are a possibility for pornographic websites, for instance considering age assurance alongside other harm mitigation mechanisms such as customisable settings (e.g., tag blacklisting), robust moderation against fair Terms of Service, proactive removal of illegal content, and robust checking for underage users who circumvent initial verification (e.g., through monitoring for contra-indicators).

5.4 **Digital library service**

My Library Portal

A local town library has introduced a digital service called *My Library Portal*. Users must have already registered at their local library and possess a valid library card to access the service.

The portal allows users to search for books by title, author, or ISBN, reserve a book, and learn whether a book is unavailable (e.g., currently on loan). Users can 'like' books to save them to a private list but they can only see the aggregate number of 'likes' for each book. User identities remain private and data on users' likes and activity is not shared with any third parties.

Library cards are typically issued through in-person processes that verify the identity and age of the user, sometimes offering a different type of card to adults and children. Therefore, any additional digital data collection for age assurance is unnecessary and disproportionate.

Concretely, this means that **device level** approaches are not applicable. Similarly, **ecosystem level** approaches, **service level** approaches and **feature level** approaches are unlikely to be necessary or proportionate.

Libraries may implement complementary harm mitigation measures, such as in-person age check, when users attempt to check out certain books (e.g., erotica), particularly where applicable rules govern access to sexually explicit material.

5.5 **Children's newsletter service**

Newskids

Newskids is a periodical newsletter service aimed at early readers that shares simplified age-appropriate stories on topics such as current events and science. The newsletter is written by a team of journalists and early learning experts.

The service is free, with subscription and unsubscription handled through a simple browser interface that collects only users' email addresses.

Services like *Newskids,* which provide content chosen and written specifically to be appropriate for all ages, have become increasingly popular as part of educational offerings or introductory news media.

Device level, ecosystem level, service level and **feature level** approaches are likely not applicable here. The content is written and vetted to ensure appropriateness for any potential visitor, and usage is unlikely to present any significant risks to children. There is no genuine need (at least on safety grounds) for the service to collect or process personal information for the purposes of verifying age.

Such services typically implement other harm mitigation measures, such as stringent authorship standards and tightly controlled (or absent) on-service advertisements. Therefore, age assurance is not needed.

Conclusion & recommendations

To safeguard children's rights in the digital environment, providers must either make services appropriate for all ages or know when users are children and cater to them. The most effective approach is to remove harmful features and functionalities to ensure the safety and privacy of all users. Alternatively, age assurance can play a key complementary role within a broader safe-by-design approach.[92]

International and European legal frameworks – particularly the GDPR, AVMSD, and DSA – provide a clear mandate: children must be able to access the digital environment in ways that respect their evolving capacities while protecting them from harm. These frameworks support a risk-based model calibrating the robustness of age assurance to the nature and severity of the risks posed by a service or feature. However, inconsistencies in implementation, uncertainty around risk classification and a narrow focus on access restriction risk undermining both children's rights and regulatory objectives. While excluding children may seem simpler than designing appropriate services, this is a cynical choice, particularly when providers continue to profit from children's engagement by choosing to implement weak age assurance measures that are not proportionate to the risks they face on their platforms.[93]

This report demonstrates that age assurance is effective and legitimate when embedded within a children's rights approach to product design, demonstrating that its value lies not in blanket age-gating, but in enabling a rights-based, proportionate approach to the digital environment. While no one-size-fits-all solution exist, the principles set out in this report must always be respected to prevent the misuse of assurance, either through overly restricting access or excessive data collection.

If age assurance is to fulfil its promise of recognising children to protect them online, it must be understood and deployed as an enabling set of tools for age-appropriate digital services, grounded in common standards, subject to meaningful oversight, and trusted by children and adults alike. Only then can it contribute to a digital environment that is not merely safer for children but genuinely designed with their rights and best interests at its core.

Recommendations
For EU and national policymakers

- **Support enforcement of existing regulation**, including the GDPR, AVMSD, and DSA, and its *Guidelines on measures to ensure a high level of privacy, safety, and security for minors online* by all online platforms and ensure that regulators have the adequate resources and capacities to enforce regulations.

- **Safeguard children's rights in all future policies and reforms of existing regulations**, including simplification proposals such as the Digital Omnibus, and ensure that protections under the UNCRC remain in place for all children until the age of 18.

- **Integrate age assurance into age-appropriate design** as a supporting measure of safety-by-design and privacy-by-design obligations, ensuring it does not replace other design changes crucial to make the online environment safer and age-appropriate for children.

- **Develop an EU norm under the DSA, based on interoperable, rights-respecting standards** such as the IEEE 2089.1 *Standard for Online Age Verification*. A formal EU recognition will provide legal certainty and clear guidance to industry, while preventing conflicts that could stifle the development of rights-respecting solutions.

- **Require independent certification, audit or conformity assessment** for age assurance tools – particularly for robust and therefore potentially invasive tools such as biometric analysis and AI-powered systems – against EU data protection and children's rights criteria.

- **Close regulatory gaps by extending protections to currently unregulated sectors like gaming and smaller platforms** through the Digital Fairness Act, and ensure consistent protections across Europe for all children, while prohibiting the most addictive and manipulative design choices that disrupt children's rights, mental health, and wellbeing.

For EU and national regulators

- **Implement and robustly enforce existing rules** – including broader requirements relating to children's protection and empowerment online – to ensure that legislation leads to changes in children's lived experience. Tech providers that fail to comply with EU rules and propose safe experiences for children should be subjected to access restrictions (Art. 51).

- **Clarify how digital services and products can ensure the best interests of the child**, including risk categorisation criteria (high, medium, low) under the DSA.

- **Coordinate across regulatory authorities at national, regional, and global level** to prevent easy circumvention of age assurance measures, building on joint actions such as the European Commission and the Digital Service Coordinators' work on pornographic platforms.[94]

For industry

- **Innovate to embed safety-by-design and privacy-by-design principles across the ecosystem**, creating spaces that are rights-respecting and age-appropriate by default. When age assurance is needed, ensure it complements these approaches rather than serving simply as an age-gating measure.

- **Show transparency and publish Child Rights Impact Assessments** and any other relevant information regarding the use of age assurance to ensure legitimacy for children and adults and enable external scrutiny of measures and their effectiveness.

- **Consult with children, parents, and child experts** in the implementation of age assurance measures to ensure tools respect the principles proposed in this report and respond to children's lived experiences.

Protecting young people online should be proactive and collaborative. Policies and platform designs must combine safety measures with education, transparency, and opportunities for young users to develop digital skills responsibly. Listening to youth voices ensures that decisions are realistic, effective, and supportive rather than overly restrictive.

PARMENAS, 23, KENYA

Acknowledgments

We are grateful to Jessica Gallissaire, Linn Høgåsen, Duncan McCann, Kim Ringmar Sylwander, Simone van der Hof and Sørine Vesth Rasmussen for their thorough review and valuable contributions that have significantly strengthened this report.

We also thank 5Rights Foundation's Youth Ambassadors who participated in the youth consultations on 'age checks' in August 2025 and on 'the digital age of majority' in November 2025. Their insights and feedback have been invaluable in understanding children's views and solutions on age assurance.

We acknowledge the support of the Lego group, whose funding made this report possible.

Endnotes

Introduction

1 5Rights Foundation. (2021a). *But how do they know it is a child?*
2 Institute of Electrical and Electronics Engineers. (2024). *IEEE 2089.1-2024 Standard for Online Age Verification*.
3 von der Leyen, U. (2024a). *Europe's choice: Political Guidelines for the next European Commission 2024-2029 (p.20)*.
4 von der Leyen, U. (2024b, July 18). *Statement at the European Parliament Plenary by President Ursula von der Leyen, candidate for a second mandate 2024-2029*.
5 von der Leyen, U. (2025a, September). *State of the Union 2025.* European Commission.
6 von der Leyen, U. (2025b, September 24). *Speech by President von der Leyen at the high-profile event 'Protecting Children in the Digital Age'*.
7 Danish Presidency of the European Union. (2025). *The Jutland declaration: Shaping a safe online world for minors*.
8 European Commission. (2025). *Guidelines on measures to ensure a high level of privacy, safety and security for minors online*.

Definitions

9 CEN-CENELEC. (2023). *Workshop Agreement CWA 18016 on age-appropriate digital services framework* (p. 10).
10 CEN-CENELEC. (2023). (p. 10).
11 CEN-CENELEC. (2023). (p. 10).
12 OECD. (2025). *The legal and policy landscape of age assurance online for child safety and wellbeing* (p. 12).

1. Children's rights in the digital environment

13 United Nations. (1989). *Convention on the Rights of the Child (UNCRC).* United Nations.
14 UN Committee on the Rights of the Child. (2013a). *General comment no. 14 (2013) on the right of the child to have his or her best interests taken as primary consideration (art. 3, para. 1)*. (p. 3, §4).
15 UN Committee on the Rights of the Child. (2013a). (p. 4, §6).
16 Livingstone, S., Cantwell, N., Özkul, D., Shekhawat, G., & Kidron, B. (2024). *The best interests of the child in the digital environment* (p. 11). Digital Futures for Children centre.
17 Livingstone, S., et al. (2024). (p19).
18 UN Committee on the Rights of the Child. (2005). *General comment no. 7 (2005), Implementing child rights in early childhood*. (pp. 8, §17).
19 UN Committee on the Rights of the Child. (2021). *General comment No. 25 (2021) on children's rights in relation to the digital environment*.
20 UN Committee on the Rights of the Child. (2013b). *General comment no. 16 (2013) on State obligations regarding the impact of the business sector on children's rights*.
21 Council of Europe. (2018). *Guidelines to respect, protect and fulfil the rights of the child in the digital environment*.
22 International Telecommunications Union. (2020). *Child Online Protection Guidelines*.
23 OECD. (2021a). *Recommendation of the Council on Children in the Digital Environment*.
24 Institute of Electrical and Electronics Engineers (IEEE). (2024). *IEEE 2089.1-2024 Standard for Online Age Verification*.

25 OECD. (2021b). *Children in the digital environment: revised typology of risks*.
26 British Standards Institution (BSI). (2018). *PAS 1296:2018 Online age checking. Provision and use of online age check services*.
27 Age Check Certification Scheme (ACCS). (2020). *ACCS 1*.
28 Institute of Electrical and Electronics Engineers (IEEE). (2021). *IEEE Standard for an Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children*.

2. Policy and regulatory context in the European Union

29 *Charter of Fundamental Rights of the European Union, Art. 24.* (2000).
30 European Commission. (2021). *EU Strategy on the Rights of the Child*.
31 European Commission. (2022a). *European strategy for a better internet for kids - BIK+*.
32 European Commission. (2021). (p. 15).
European Commission. (2022b). *A Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+)*. (p. 10).
33 European Commission. (2024a). *Age assurance for digital service providers: self-assessment tool*.
34 European Commission. (2024b). *Research report: Mapping age assurance typologies and requirements*.
35 European Commission. (2023). *European Declaration on Digital Rights and Principles*.
36 For the full list, see European Commission. (2024c). *New Better Internet for Kids Strategy (BIK+): Compendium of EU Formal texts concerning children in the digital world – 2024 edition*.
37 *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. (2016).
38 See also The Swedish Authority for Privacy Protection, The Ombudsman for Children in Sweden, & The Swedish Media Council. (2021). *Stakeholder Guide: The Rights of Children and young people on digital platforms*. Agencia Española Proteccion Datos (AEPD). (2023). *Decalogue of principles - Age verification and protection of minors from inappropriate content*.
39 Commission Nationale de l'Informatique et des Libertés (CNIL). (2021). *8 recommendations to enhance the protection of children online*.
40 Coimisinéir Cosanta Sonraí (Data Protection Commission of Ireland – DPC). (2021). *Fundamentals for a Child-Oriented Approach to Data Processing*.
41 European Data Protection Board. (2025a). *Statement 1/2025 on Age Assurance*.
42 *Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive)*. (2010).
43 Coimisiún na Meán. (2024). *Online Safety Code*.

3. Principles for implementing age assurance

44 *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)*. (2022).
45 European Commission. (2025). *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*.
46 OECD. (2021b). *Children in the digital environment: revised typology of risks*.
47 European Commission (2025). (§37).
48 European Data Protection Board. (2025). *Statement 1/2025 on Age Assurance* (p. 2, §2.1).
49 5Rights Youth Ambassadors. (2025a). *Youth consultation on age checks* (carried out by 5Rights Foundation).
50 Hilton, Z., & King, H. (2021). *Making age assurance work for everyone: inclusion considerations for age assurance and children*.
51 5Rights Youth Ambassadors. (2025b). *Youth consultation on the digital age of majority* (carried out by 5Rights Foundation).
52 5Rights Foundation. (2021a). (p. 48). See also CEN-CENELEC. (2023). (§ 8.3). See also OECD. (2024). (p. 31).

53 For more information on the need to conduct an assessment see Agencia Española Protección Datos (AEPD). (2024). *Technical note: A safe internet by default for children and the role of age verification* (p.11). See also European Data Protection Board (EDPB). (2025). (§2.2). See also European Commission. (2025). (§31). See also Sas, M., & Mühlberg, J. (2024). *Trustworthy age assurance?*.

54 On CRIAs see Digital Futures Commission. (2021). *Child Right Impact Assessment: A tool to realise children's rights in the digital environment*. See also Livingstone, S., & Pothong, K. (2025). *Child Rights Impact Assessment: A Policy Tool for a Rights Respecting Digital Environment*. Policy & Internet, 17(3).

55 European Commission. (2024b). (§5.10).

56 European Data Protection Board. (2025). (§2.4).

57 5Rights Foundation. (2021a). (p. 48).

58 European Commission. (2025). (§39).

59 European Commission. (2025). (§2.3 & 2.8).

60 European Data Protection Board. (2025). (§ 2.3).

61 European Data Protection Board. (2025). (§ 2.9).

62 See for instance Renaissance Numérique. (2022). *Age assurance online – Working towards a proportionate and European approach*.

63 Agencia Española Protección Datos (AEPD). (2023). *Technical Note: Description of the proofs of concept of systems for age verification and protection of minors from inappropriate content*.

64 Agencia Española Protección Datos (AEPD). (2024). *Technical Note: A safe internet by default for children and the role of age verification*.

65 Gorin, J., Biéri, M., & Brocas, C. (2022). *Demonstration of a privacy-preserving age verification process*.

66 Institute of Electrical and Electronics Engineers (IEEE). (2024).

67 International Organization for Standardization (ISO). (2025). *ISO/IEC 27566-1:2025: Information security, cybersecurity and privacy protection — Age assurance systems*.

68 European Commission. (2025). (§40).

69 European Data Protection Board. (2025). (§2.5).

70 5Rights Foundation. (2021a). (p. 49). See also CEN-CENELEC. (2023). (§8.3).

71 5Rights Foundation. (2021a). (p. 48).

72 5Rights Foundation. (2021a). (p. 51).

73 European Commission. (2025). (§48).

74 See for instance: DRCF (2023), *Measurement of Age Assurance Technologies*.

75 5Rights Foundation, (2025b).

76 5Rights Foundation. (2021a). (p. 49).

77 European Commission. (2025). (§34). Some authors have started to examine potential performance metrics for deployed systems, for example in the ACCS recommendations to the ICO: Allen, T., McColl, L., Walters, K., & Evans, H. (2022). *Measurement of Age Assurance Technologies*.

78 See for instance 5Rights Foundation. (2021b). *Tick to Agree – Age appropriate presentation of published terms*.

79 CEN-CENELEC. (2023). (§8.3). See also 5Rights Foundation. (2021a). (p. 50).

80 Participation of children is recognised in European Commission. (2025). (§35). See also European Commission (2024b). (§5.10).

4. **A Risk-based spectrum of approaches**

81 5Rights Foundation. (2021a). (p. 49).

82 5Rights Foundation. (2021a). (p. 11).

83 European Commission. (2024b). See also European Commission. (2025). (§36).

84 European Commission. (2025). (§37). See also Coimisiún na Meán. (2024). (§12.10).

85 5Rights Foundation. (2021a). (p. 29).

86 Data Protection Commission of Ireland (DPC). (2023). Quoted in Livingstone, S., Nair, A., Stoilova , M., van der Hof, S., & Caglar, C. (2024). *Children's Right and Online Age Assurance Systems*. The International Journal of Children's Rights.

87 Digital Regulation Cooperation Forum (DCRF), & Revealing Reality. (2022). *Families' attitudes towards age assurance* (p. 16). Ofcom. See also Luria, M., & Bhatia, A. (2025). *What Kids and Parents Want: Policy Insights for Social Media Safety Features*. Center for Democracy & Technology (CDT).

88 Livingstone, S., Nair, A., Stoilova , M., van der Hof, S., & Caglar, C. (2024).
89 Coimisiún na Meán. (2024). (§12.10). See also European Commission. (2025). (§47b, 52).

5. Case in applying age assurance tools in practice

90 van der Hof, S., & Lievens, E. (2017). *The Importance of Privacy by Design and Data Protection Impact Assessments in Strengthening Protection of Children's Personal Data Under the GDPR*. Communications Law, 23(1).
91 We define microtransactions as small-value digital transactions made cumulatively over time, compared to a single upfront cost.

Conclusion & recommendations

92 OECD. (2024). (p.6).
93 Livingstone, S., Nair, A., Stoilova, M., van der Hof, S., & Caglar, C. (2024). (p.732).
94 European Commission. (2025b). *The European Board for Digital Services launches a coordinated action to reinforce the protection of minors as regards pornographic platforms*.

5RIGHTS FOUNDATION

@5RightsFound
www.5rightsfoundation.com