ETSI TR 104 077-1 V1.1.2 (2024-12)

Human Factors (HF);
Age Verification Pre-Standardization Study
Part 1: Stakeholder Requirements

Reference
RTR/HF-00301567

Keywords
age verification, requirements, stakeholders

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Human Factors (HF).

The present document is part 1 of a multi-part deliverable covering Age Verification Pre-Standardization Study, as identified below:

Part 1: "Stakeholder Requirements";

Part 2: "Solution and Standards Landscape";

Part 3: "Proposed Standardization Roadmap".

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

The present document outlines stakeholder requirements for age verification, essential for developing a standardized approach to age verification and age estimation solutions. The aim is to align efforts across various sectors and jurisdictions, ensuring the protection of minors online while complying with legal and regulatory requirements.

For underage users of internet services, the present document highlights the need for systems that reliably verify age using secure methods that protect personal data. It emphasizes the implementation of Privacy-Preserving verification methods to ensure anonymity and data minimization, collecting only the essential data necessary for age verification. The processes should be seamless, avoiding barriers for users.

Parents of underage users need systems that facilitate obtaining and verifying parental consent, ensuring both parents' involvement where applicable. The present document stresses transparency, providing clear, age-appropriate information about data collection and usage. Tools should allow parents to manage their children's online activities and revoke consent if necessary. Additionally, parents should be informed about safe online practices and the importance of privacy.

Adult users require assurances that any data collected during age verification will be protected and not misused. Clear information about the age verification process and data handling practices is essential for maintaining trust.

Providers of age verification services and national authorities have to adhere to GDPR [i.4], the Digital Services Act, and other relevant legal frameworks. The present document advocates for developing interoperable systems that work across various platforms and jurisdictions, implementing robust security measures to protect data during transmission and storage. Continuous oversight and updates to age verification methods are crucial to address emerging challenges.

Service providers subject to age verification obligations have to ensure the content provided is suitable for the verified age group. Compliance with national and international regulations regarding age-restricted content and services is mandatory. Age verification should not hinder user experience and be integrated smoothly into the service. Robust parental control settings should be integrated to manage access to content.

The plan for standardization involves establishing unified standards with comprehensive guidelines detailing the technical and procedural requirements for age verification systems. Encouraging the development of interoperable systems that can be easily adopted by service providers and verified by national authorities is important. Compliance with GDPR [i.4], eIDAS2 [i.2], and other relevant laws provides a legal framework for data protection and user privacy. Regular audits and compliance checks help maintain the integrity of age verification processes.

Collaboration among stakeholders, including service providers, regulatory bodies, parents, and user advocacy groups, ensures solutions meet diverse needs and concerns. Educational campaigns inform stakeholders about the importance of age verification and effective tool usage. Establishing feedback mechanisms to gather input from stakeholders, staying updated with technological advancements, and incorporating innovative solutions to address new challenges are essential steps.

Introduction

The present document aims to establish and analyse stakeholder requirements for age verification, laying the groundwork for future European standards in this field as requested in the Digital Services Act. Regulation (EU) 2022/2065 [i.1] mandates the development of standards for targeted measures to protect minors online (Article 44 (j)), including age verification systems and parental control tools (Article 35 (j)). However, achieving a unified European solution for age verification might be challenging due to disparate national systems. Thus, establishing comprehensive requirements for age verification and parental controls, as well as standardized interfaces for service providers to access verified age data, is crucial for protecting minors online. International organizations like ITU/IEC, national standards bodies, and the euConsent EU-funded project have explored age verification and protection of minors. Their research provides a basis for assessing current solutions and identifying gaps.

While the euConsent project explored age verification in depth, its solutions primarily focus on agency-supported verification, leaving significant questions unanswered. Specifically, the seamless sharing of verified age data among parents, minors, and service providers remains underexplored.

The present document will focus on identifying and understanding the requirements of all stakeholders with an interest in age verification. The present document aims at understanding the needs of different stakeholder groups, including children, parents, service providers, and society as a whole, in their use of age-verified information, and to define the requirements of stakeholders comprehensively, ensuring future standards are practical and meet the needs of all parties involved.

1 Scope

The present document identifies stakeholder requirements for age verification.

NOTE: The present document may assist in providing the groundwork for defining standards as outlined in the Digital Services Act [i.1]. Its purpose is to establish the foundation for developing European standards in age verification and protecting minors online.

The present document presents the analysis of requirements of identified stakeholders in the age verification process for whom accurate age information is essential to their service access or to their business operation.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long-term validity.

The following referenced documents are not necessary for the application of the present document, but they assist the user with regard to a particular subject area.

[i.1] 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).

[i.2] Regulation (EU) 2024/1183 of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.

[i.3] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[i.4] 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).

[i.5] ETSI TS 119 461 (V1.1.1):"Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects".

[i.6] ISO/IEC WD 27566-1: "Information security, cybersecurity and privacy protection Age assurance systems. Framework Part 1: Framework".

[i.7] UNICEF: "Convention on the Rights of the Child".

[i.8] OFCOM: "Quick guide to children's access assessments".

[i.9] OFCOM: "Guidance on age assurance and other Part 5 duties for service providers publishing pornographic content on online service".

[i.10] CNIL - Recommendation 7: "Check the age of the child and parental consent while respecting the child's privacy". (August 2021).

[i.11] CNIL - Online age verification: "Balancing privacy and the protection of minors". (September 2022).

[i.12] DPC - Front and Centre: "The Fundamentals for a Child-Oriented Approach to Data Processing". (December 2021).

[i.13] AEPD - Decalogue of principles: "Age verification and protection of minors from inappropriate content". (December 2023).

[i.14] Draft Spanish law on the protection of children and adolescents in the digital environment.

[i.15] ICO: "Age assurance for the Children's code". (January 2024).

[i.16] BSI PAS 1296:2018: "Online age checking; Provision and use of online age check services; Code of Practice". (March 2018).

[i.17] IEEE 2089™-2021: "IEEE Standard for an Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children".

[i.18] IEEE 2089.1™-2024: "IEEE Draft Standard for Online Age Verification".

[i.19] NIST: "Face Analysis Technology Evaluation (FATE) Age Estimation & Verification".

[i.20] CNIL: "Demonstration of a privacy-preserving age verification process". (June 2022).

[i.21] AEPD: "Technical note - Description of the proofs on concept for systems for age verification and protection of minors from inappropriate content". (December 2023).

[i.22] Digital Regulation Cooperation Forum (UK): "Families' attitudes towards age assurance". (October 2022).

[i.23] Measurement of Age Assurance Technologies - Part Two (August 2023): "Measurement of Age Assurance Technologies. A Research Report for the Information Commissioner's Office (ICO)".

[i.24] Yoti: "Facial Age Estimation White Paper".

[i.25] 5Rights Foundation: "But how do they know it's a child?". (October 2021).

[i.26] The Center for Growth and Opportunity: "Keeping Kids Safe Online: How Should Policymakers Approach Age Verification?". (June 2023).

[i.27] UNICEF: "Digital Age Assurance Tools and Children's Rights Online across the Globe: A Discussion Paper". (April 2021).

[i.28] Praesidio Safeguarding: "Making age assurance work for everyone: inclusion considerations for age assurance and children".

[i.29] The Age Verification Providers Association: "Privacy; a foundational concept for age verification". (March 2024).

[i.30] Centre for Information Policy Leadership: "Age Assurance and Age Verification Tools: Takeaways from CIPL Roundtable". (March 2023).

[i.31] Centre for Information Policy Leadership: "A Multi-Stakeholder Dialogue on Age Assurance". (March 2024).

[i.32] Digital Trust & Safety Partnership: "Age Assurance: Guiding Principles and Best Practices". (September 2023).

[i.33] euCONSENT / Simone van der Hof: "Methods for Obtaining Parental Consent and Maintaining Children Rights". (September 2021); "Age assurance and age appropriate design: what is required?". (November 2021).

[i.34] Family Online Safety Institute: "Making Sense of Age Assurance: Enabling Safer Online Experiences". (November 2022).

[i.35] Future of Privacy Forum: "Unpacking Age Assurance: Technologies and Tradeoffs". (June 2023).

[i.36] 36Age Check Certification Scheme: "Global Age Assurance Standards". Summit 2024.

[i.37] UK: "Online Safety Act 2023".

[i.38] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and repealing Regulation (EEC) No 339/93.

[i.39] United Nations Convention on the Rights of the Child (UNCRC), 1989.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

age: length of time that a person or thing has existed

age assurance: methods used to determine the age or age range of an individual, including age verification, estimation, and self-declaration

age check exchange: online gateway where age check providers and parties assess user attributes

NOTE: See PAS 1296:2018 [i.16].

age check provider: organization responsible for establishing and maintaining a person's identity attributes

NOTE: See PAS 1296:2018 [i.16].

age estimation: process to determine an individual's likely age range by analysing inherent features or behaviours

age gate: technical measure that restricts access to digital content for those who are not of the appropriate age

Age Verification (AV): process to determine an individual's age or age range

attestation of attributes validation: process of verifying and confirming that an attestation of attributes is valid

NOTE: See eIDAS2 definition [i.2].

attribute: characteristic, quality, right or permission of a natural person

NOTE: See eIDAS2 definition [i.2].

authentication: electronic process that enables the confirmation of the electronic identification of a natural or legal person or the confirmation of the origin and integrity of data in electronic form

NOTE: See eIDAS2 definition [i.2].

authentic source: repository or system, held under the responsibility of a public sector body or private entity, which contains and provides attributes about a natural and that is considered to be a primary source of that information or recognized as authentic in accordance with Union or national law, including administrative practice

NOTE: See eIDAS2 definition [i.2].

child: natural person under 18 years of age

children's rights: rights as outlined in the United Nations Convention on the Rights of the Child (UNCRC) [i.39], focusing on ensuring child welfare and protection

conformity assessment body: entity as defined in Article 2, point 13, of Regulation (EC) No 765/2008 [i.38], which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a service provider and the services it provides

consent: clear and informed indication that a data subject agrees to data processing

contra-indicator: information that contradicts a claimed age attribute or identity, raising doubts about its validity

digital identity document: identity document that is issued in a machine-processable form, that is digitally signed by the issuer, and that is in purely digital form

NOTE 1: Machine-processable, in this case, does not include optical scanning and processing of a physical identity document.

NOTE 2: A digital identity document can be contained in a physical identity document, e.g. an eMRTD contained in a passport or national identity card.

NOTE 3: The "electronic identification" part of a passport or national identity card is sometimes called "electronic identity" or even "eID". In the present document, this part of a passport or national identity card is a digital identity document.

electronic attestation of attributes: attestation in electronic form that allows the authentication of attributes describing features, characteristics or qualities of a natural or legal person or of an entity, or a natural person representing a legal person, or of an object

NOTE: See eIDAS2 definition [i.2].

electronic identification: process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing another natural person or a legal person

NOTE: See eIDAS2 definition [i.2].

electronic Identification means (eID means): material and/or immaterial unit containing person identification data and which is used for authentication for an online service or, where appropriate, for an offline service

NOTE: See eIDAS2 definition [i.2].

eID scheme: governance model and technical specifications allowing interoperability between eID means from different eID providers

(identity) evidence: information or documentation provided by the applicant or obtained from other sources, trusted to prove that claimed identity attributes are correct

NOTE: See ETSI TS 119 461 [i.5].

identity: attribute or set of attributes that uniquely identify a person within a given context

NOTE: See ETSI TS 119 461 [i.5].

identity matching/identification: process where person identification data, or electronic identification means are matched with or linked to an existing account belonging to the same person

NOTE: See ETSI TS 119 461 [i.5].

identity proofing context: external requirements affecting the identity proofing process, given by the purpose of the identity proofing, the related regulatory requirements, and the resulting restrictions on the selection of attributes and evidence and on the identity proofing process itself

NOTE: See ETSI TS 119 461 [i.5].

identity proofing (process): process by which the identity of an applicant is verified by the use of evidence attesting to the required identity attributes

NOTE: See ETSI TS 119 461 [i.5].

indicators of confidence: quantitative, qualitative or descriptive measure of the correctness and accuracy to which an age assurance attribute can be stated to relate to a natural person

NOTE: See ISO 27566-1 (Committee Draft) [i.6].

legitimate evidence holder: person for whom the evidence is issued

NOTE: See ETSI TS 119 461 [i.5].

Level of Identity Proofing (LoIP): confidence achieved in the identity proofing

liveness detection: measurement and analysis of anatomical characteristics or involuntary or voluntary reactions, to determine if a biometric sample is being captured from a living subject present at the point of capture

parental consent: consent from someone with parental authority over children under a specified age

parental controls: filtering settings to monitor children's online activity and protect them from harmful content

personal data: any information as defined in Article 4, point (1), of Regulation (EU) 2016/679 [i.4]

physical identity document: identity document issued in physical and human-readable form

EXAMPLE: The printed (non-digital) representation of passport.

NOTE: See ETSI TS 119 461 [i.5].

profiling: automated processing of personal data to evaluate personal aspects like work performance or behaviour

pseudonym: fictitious identity that a person assumes for a particular purpose, which differs from their original or true identity

NOTE 1: Pseudonym identity can, as opposed to an anonymous identity, be linked to the person's real identity.

NOTE 2: See ETSI TS 119 461 [i.5].

pseudonymization: process of processing data in a way that cannot be attributed to an individual without additional information

relying party: natural or legal person that relies upon electronic identification, European Digital Identity Wallets or other electronic identification means, or upon a trust service on an age assurance assertion or claim to make an age-related eligibility decision

NOTE: See eIDAS2 definition [i.2].

remote identity proofing: identity proofing process where the applicant is physically distant from the location of the identity proofing

NOTE: See ETSI TS 119 461 [i.5].

selective disclosure: capability of the application that enables the user to present a subset of attributes

EXAMPLE: EUDI Wallet and an Electronic Attestation of Attributes (EAA) with the attributes first name, last name, birth date, and address. The user can for example selectively disclose only its first name.

strong user authentication: authentication based on the use of at least two authentication factors from different categories of either knowledge, something only the user knows, possession, something only the user possesses or inherence, something the user is, that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data

NOTE: See eIDAS2 definition [i.2].

unique identifier: unique data used to represent a person's identity and associated attributes

unlinkability: lack of information required to connect the user's selectively disclosed attributes beyond what is disclosed

NOTE 1: Verifier unlinkable means that one or more verifiers cannot collude to determine if the selectively disclosed attributes describe the same identity subject.

NOTE 2: Issuer unlinkable means that one or more issuers cannot collude to determine if the selectively disclosed attributes describe the same identity subject.

NOTE 3: Fully unlinkable means that no party can collude to determine if the selectively disclosed attributes describe the same identity subject.

NOTE 4: Multi-show unlinkability means that a (Q)EAA can be used for multiple presentations, which cannot be used to connect the user's selectively disclosed attributes.

NOTE 5: The opposite of multi-show unlinkability means that, i.e. a (Q)EAA can only be used once for a presentation, since the (Q)EAA will thereafter reveal information that can be used for linkability.

untraceability: property that ensures that an age assurance attribute used by a natural person in a particular context cannot be traced to that natural person by a relying party

NOTE: Untraceability applies to other third parties not being able to trace back to the age assurance service provider, but individuals would be aware of the age assurance service provider to be able to exercise their data rights.

validation: part of an identity proofing process that determines whether or not attributes are validated by the presented evidence and whether or not the evidence is genuine, authoritative, and valid

Zero-Knowledge Proof (ZKP): method by which the user (prover) can prove to the relying party (verifier) that a given statement is true while the user does not provide any additional information apart from the fact that the statement is true

NOTE 1: There are special-purpose ZKPs that can only prove very specific statements (knowledge of a pre-image of a hash or knowledge of a signature under a specific digital signature scheme) and general-purpose or programmable ZKPs that allow to prove any statement. Programmable ZKPs usually involve a compiler from some programming language that describes the statement to be proved (program returns a certain public value upon correct execution on a private input) into a ZKP proving and verification program.

NOTE 2: A ZKP protocol should meet the following three criteria: Completeness (if the statement is true then a user can convince a verifier), soundness (a fraudulent user cannot convince a verifier of a false statement beyond negligible probability - how small is a parameter choice, 2^{-128}), and zero-knowledge (the interaction only reveals if a statement is true and nothing else beyond what can trivially be inferred from the statement itself).

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AE	Age Estimation
AEPD	Agencia Española de Protección de Datos
AI	Artificial Intelligence
AV	Age Verification
CCPA	California Consumer Privacy Act
CIPL	Centre for Information Policy Leadership
CNIL	Commission Nationale de l'Informatique et des Libertés
COPPA	Children's Online Privacy Protection Act
CRIA	Children's Rights Impact Assessment
DPC	Data Protection Commission
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EAA	Electronic Attestation of Attributes
EDPB	European Data Protection Board
eID	electronic Identification
eIDAS	electronic Identification, Authentication and Trust Services
eMRTD	electronic Machine-Readable Travel Document
EUDI	European Digital Identity
FOSI	Family Online Safety Institute
FPR	False Positive Rate
FTC	Federal Trade Commission
ICO	Information Commissioner's Office

IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
ISS	Information Society Services
LO	Ley Orgánica
LoIP	Level of Identity Proofing
MAE	Mean Absolute Error
NGO	Non-Governmental Organization
NIST	National Institute of Standards and Technology
PAS	Publicly Available Specification
QEAA	Qualified Electronic Attestation of Attributes
QR	Quick Response
TPR	True Positive Rate
UKAS	United Kingdom Accreditation Service
UNCRC	United Nations Convention on the Rights of the Child
URL	Uniform Resource Locator
VoCO	Voice Controlled Operations
VPN	Virtual Private Network
ZKP	Zero-Knowledge Proof

4 Age Verification Overview

Age assurance is required across a wide range of online industry sectors. There are guides being made available by government organizations to aid online industries in ensuring they are complying to regulations. Ideally, the online industries keep risks and safety measures under regular review.

For example:

- Betting and Gambling
- Music Streaming Sites
- Video Sharing Platforms
- Adult websites
- Advertising platforms
- Social Media
- Computer Gaming
- Online Pharmacies
- Knives and acid sales
- Cannabinoid sales
- Supermarkets
- Fast food delivery
- Vaping sites
- Dating sites

These requirements arise for a number of common reasons:

1) Child Protection e.g. risk management when adults interact with children online;

2) Data Protection e.g. to implement Article 8, GDPR [i.4];

3) Age-restricted products e.g. vaping, alcohol;

4) Age-restricted services e.g. gambling;

5) Age-restricted content e.g. pornography, violent games.

Table 1

	Child Protection	Data Protection	Age-restricted products	Age-restricted services	Age-restricted content
Betting and Gambling		X		X	
Music Streaming Sites					
Video Sharing Platforms	X	X			X
Adult websites	X	X			X
Advertising platforms		X	X		
Social Media	X	X		X	X
Computer Gaming	X	X			
Online Pharmacies		X	X		
Knives and acid sales		X	X		
Cannabinoid sales		X	X		
Supermarkets		X	X		
Fast food delivery		X	X		
Vaping sites		X	X		
Dating sites	X	X		X	X

5 Stakeholders categorization

At its broadest, the stakeholders in this process will include almost everyone who makes use of the internet. However, some stakeholders will require particular attention and will be the principal target of the present document. It should be noted that there is guidance available to aid specific industries to enable them to comply age verification regulations., though these are often by specific national laws. Amongst these stakeholders, the following ones have been identified:

- Underage users of internet services and recipients of information groups.
- Parents of underage users.
- Adult users of internet services and recipients of information groups.
- Providers of age verification services and national authorities providing age verification solutions.
- Service providers which need age information to ensure that minors receive only adequate information and services as defined/required by parents or by legal restrictions.

The stakeholders will have one or more of the following requirements covered:

- Accurate age attribution: Age verification systems are needed to attribute correct age information to children, using reliable identification.
- Adequate content delivery: Use accurate age information to provide appropriate content/services to minors as set by parents or law.
- Age-appropriate content: Ensure that information and services accessible to underage users are suitable for their age group.
- Compliance: Ensure solutions comply with national and international regulations, such as the EU Digital Services Act [i.1], UK Online Safety Act [i.37] and eIDAS2 [i.2].

- Consent and understanding: Ensure that age verification processes are explained clearly, helping minors comprehend the need for such measures.
- Cross-platform consistency: Maintain consistent age settings across devices and platforms.
- (Cyber) security: age information may not be tampered with or modified during communication and internet access.
- Data security: Implement strict security protocols to safeguard the collection, storage, and transmission of age-related data.
- Flexible implementation: Enable a flexible implementation of age settings to cater to different service requirements.
- Interoperability: Enable systems to work seamlessly with various platforms, including those managed by national authorities.
- Legal compliance: Ensure age-related content delivery adheres to regional and international laws.
- Monitoring tools: Provide parents with transparent monitoring options for their children's internet usage while respecting minors' privacy.
- Parental control integration: Seamlessly integrate parental control settings with existing age verification systems.
- Parental control settings: Offer features to define rights, such as in-app purchases or accessing restricted content.
- Privacy: Protect information about minors and adults and their rights , which may only be used by service providers on a need-to-know basis.
- Service provider adherence: Allow the possibility to check if individual service providers fulfil their obligation defined in the regulation (as the Digital Services Act [i.1]).
- Transparency and accountability: Make service operations transparent and hold providers accountable for meeting stakeholder requirements
- Usability: When accessing the internet, age verification should not delay the communication or require continuous interaction by minors or adults with the service and/or their end user device.
- User experience: Provide easy-to-use interfaces for age verification that minimize barriers and support inclusivity.

Table 2 identifies the main requirements of the above identified stakeholders.

Table 2

	Underage users	Parents	Adults	Providers of Age Verification	Service Providers
Accurate age attribution		X	X		
Adequate content delivery					X
Age-appropriate content	X				
Compliance				X	
Consent and understanding	X	X	X		
Cross-Platform Consistency		X			
(Cyber) Security				X	X
Data Security	X		X	X	
Flexible implementation					X
Interoperability				X	
Legal compliance					X
Monitoring tools		X			
Parental Control Integration					X
Parental Control Settings		X			
Privacy	X		X		
Service Provider Adherence					X
Transparency and accountability				X	
Usability	X		X		
User experience	X				

6 Age Verification sources

6.1 Method for analysing and collecting information

The information analysed in the present document aims to identify common trends and select relevant ones for the following TR, addressing stakeholder requirement for age verification.

The analysis consists of the following stages:

- the analysis against any source of information in reading sheets using the general methodology included in clause 6.2.1;
- the analysis across the sources of information, for each requirement of the methodology against reading sheets. This aims to derive trends or identify gaps; and
- the conclusion that identifies the relevant information for following developments (see clause 7).

The present document surveys the technologies, legislations, specifications, guidelines, and standards related to or used for age verification. Information comes from sources such as national agencies developing requirements, research and academic environments, and relevant existing specifications and Age Assurance regulation revision.

6.2 Information collected on Age verification and estimation

6.2.1 Introduction

To define stakeholder requirements in a documented way, analysis of Age Assurance reading and resource list. Last Updated: 30 June, 2024.

The present clause introduces each document analysed by the STF that have been analysed through the perspective of the reading sheet.

The reading sheets are not a detailed description/comprehensive analysis of the referenced documents but try to summarize the main points. Readers are encouraged to consult the references provided at the beginning of the reading sheets if interested in more info. Some of the main requirements from the referenced document are restated for information in the present document.

6.2.2 Regulatory Guidance

6.2.2.1 France

6.2.2.1.1 CNIL - Recommendation 7: Check the age of the child and parental consent while respecting the child's privacy (August 2021)

Title	Recommendation 7: Check the age of the child [i.10]
Organization	CNIL
Source (link, URL…)	https://www.cnil.fr/en/recommendation-7-check-age-child-and-parental-consent-while-respecting-childs-privacy
Country	France
Short description	
The document addresses the complexities and necessities surrounding age verification and parental consent for children accessing online services. It emphasizes the need to balance child protection with privacy rights, particularly the principle of online anonymity. Key points include: • Age Verification: Existing methods, such as facial recognition, are often criticized for mass data collection, potentially breaching data protection laws. Less intrusive methods like self-declaration or email verification are noted as easily circumvented. • Parental Consent: It is stressed that consent ideally should come from both parents, regardless of relationship status. However, in some cases, consent from just one parent may suffice, based on the child's best interests. • Legal Framework: Guidelines from the EDPB highlight the GDPR's [i.4] requirements for online service providers to verify age and obtain parental consent using reasonable efforts and appropriate technologies. • Proposed Solutions: The European Commission is exploring an interoperable technical infrastructure using electronic identification means to implement these protections effectively across EU states. The CNIL emphasizes several principles for age and consent verification systems: • Proportionality (using technologies appropriate to the risk). • Minimization (collecting only necessary data). • Robustness (especially for high-risk processing like targeted advertising). • Simplicity (user-friendly solutions). • Standardization (industry-wide compliance and certification). There is also encouragement for third-party verification systems and ongoing monitoring and support for compliant solutions by regulatory bodies like the CNIL and the European Commission. While the document acknowledges the challenges and absence of a perfect solution, it outlines a framework emphasizing legal compliance, technological feasibility, and protection of children's privacy in the digital age.	
Stakeholder	**Requirements**
Underage users of internet services and recipients of information groups.	• Implement an age verification system that minimizes data collection and respects children's privacy. • Implement privacy-preserving age verification methods, to ensure children's privacy is protected while effectively verifying their age. • Require consent from both parents or legal guardians before allowing children to access certain online services. • Allow consent from one parent, if it is in the child's best interests. • Ensure that any data collected for age and consent verification is proportional to the risk and purpose, adhering to the principle of data minimization. • Develop and promote user-friendly, standardized systems for age and consent verification across the industry, increasing the likelihood of proper usage by underage users.

Stakeholder	Requirements
Parents of underage users.	• Create mechanisms to obtain and verify consent from both parents or legal guardians, with allowances for single-parent consent in the child's best interests. • Develop and promote user-friendly, standardized systems for age and consent verification across the industry, increasing the likelihood of proper usage by parents. • Create mechanisms for parents to easily revoke or manage their consent at any time, with changes taking effect promptly across all relevant online services.
Adult users of internet services and recipients of information groups.	• Ensure that consent mechanisms for data processing are clear, simple, and user-friendly, allowing adults to easily understand and actively control their data. • Ensure that any collected data is anonymized or deleted after verification is complete. • Implement an age verification system that minimizes data collection and respects users' privacy. • Provide easy-to-access options for users to review and withdraw their consent at any time without complex procedures.
Providers of age verification services and national authorities providing age verification solutions.	• Implement privacy-preserving age verification methods that are effectively yet minimally invasive. • Develop secure systems for obtaining and verifying parental consent, ideally requiring dual consent from both parents but allowing for exceptions when necessary. • Ensure all systems comply with GDPR [i.4] and other relevant legal frameworks, following guidelines set by regulatory bodies such as the EDPB. • Develop and implement an interoperable technical infrastructure for age verification, as explored by the European Commission, using standardized electronic identification means across EU States. • Establish continuous monitoring and support systems with oversight from regulatory bodies like the CNIL and the European Commission.
Service providers which need age information to ensure that minors receive only adequate information and services as defined/required by parents or by legal restrictions.	• Develop a robust system for obtaining and managing parental consent, to ensure it is legitimate and in line with the child's welfare. • Ensure all practices related to age verification and parental consent comply with GDPR [i.4] and other relevant legal frameworks, following guidelines set by regulatory bodies such as the EDPB. • Implement mechanisms to tailor the content and services provided based on verified age information, ensuring minors only gain access to appropriate material. • Conduct regular audits and continuous monitoring of age verification processes and content management systems to ensure compliance and effectiveness.

6.2.2.1.2 CNIL - Online age verification: balancing privacy and the protection of minors (September 2022)

Title	Online age verification: balancing privacy and the protection of minors [i.11]
Organization	CNIL
Source (link, URL…)	https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors
Country	France

Short description

The CNIL has evaluated age verification systems on the internet, focusing on their application to pornographic sites, which are legally required to verify users' ages. The CNIL finds current methods to be both intrusive and easily circumvented, urging for more privacy-respecting alternatives.
They suggest the primary challenge in online age verification lies in accurately identifying users without compromising their privacy. Identification processes can link sensitive personal data to online activities, raising significant privacy concerns. While some online activities inherently require identity verification, others, like browsing, should ideally remain anonymous. Overly intrusive age verification can hinder users' privacy and limit access to legitimate content.
The CNIL emphasizes education on cyber practices for children, parents, and educators to foster better digital habits. It recommends a framework for age verification based on six principles: minimization, proportionality, robustness, simplicity, standardization, and third-party involvement. Central to the CNIL's approach is the preference for user-controlled systems rather than centralized ones, advocating for parental control mechanisms to manage access to inappropriate content.
French and European laws mandate age verification for certain online services, necessitating robust identity proof due to legal and payment requirements. However, the CNIL cautions against excessive age verification demands that could reduce access to freely accessible sites.
For pornographic sites, the CNIL insists on strict adherence to legal requirements for age verification, prohibiting simple self-declaration of age and suggesting independent third-party involvement to prevent the direct collection of user data by the site publishers. The CNIL's recommendations aim to balance protecting minors from inappropriate content while safeguarding users' privacy.
To achieve this, the CNIL suggests:

- Utilizing trusted third-party systems for age verification.
- Avoiding direct identity documentation collection by site publishers.
- Employing cryptographic methods to verify age without revealing other personal data.

The document suggests that current age verification solutions are flawed, often by passable via VPNs or misuse of identity documents. The CNIL encourages the development of more reliable, privacy-preserving systems and proposes certification for third-party providers to ensure GDPR [i.4] compliance. The CNIL also explores privacy-friendly verification systems, like zero-knowledge proofs, which verify age without disclosing identity, highlighting the importance of independent third parties in this process.

Stakeholder	Requirements
Underage users of internet services and recipients of information groups.	• Use trusted third-party verification systems, rather than the site publishers themselves. This helps ensure that users' personal data is not directly shared with or misused by the website publishers. • Educate and inform underage users about safe online practices and the importance of privacy. • Collect only the information necessary to verify age without gathering excessive or unrelated personal data, helping to protect the privacy of underage users. • Collect only the necessary data required to verify age.
Parents of underage users.	• Educate and inform parents about safe online practices and the importance of privacy. • Incorporate systems that include user-controlled mechanisms, such as parental control tools, to manage and restrict access to inappropriate content for minors. • Provide parents with and encourage them to use alternative age verification methods that do not require personal identification documents. • Encourage parents to use services from certified third-party providers for verifying their children's age.
Adult users of internet services and recipients of information groups.	• Use trusted third-party verification systems, rather than the site publishers themselves. This helps ensure that users' personal data is not directly shared with or misused by the website publishers. • Educate and inform adult users about safe online practices and the importance of privacy. • Collect only the necessary data required to verify age.

Stakeholder	Requirements
Providers of age verification services and national authorities providing age verification solutions.	• Ensure your age verification system is certified and adheres to standardized procedures to ensure reliability and security. • Utilize systems like zero-knowledge proofs to verify age without disclosing personal details. • Employ privacy-preserving techniques, such as cryptographic methods, that can confirm a user's age without revealing any other personal information.
Service providers which need age information to ensure that minors receive only adequate information and services as defined/required by parents or by legal restrictions.	• Use trusted third-party verification systems, rather than the site publishers themselves. This helps ensure that users' personal data is not directly shared with or misused by the website publishers. • Prevent site publishers from directly collecting identity documents (such as passports) from users for age verification processes.

6.2.2.2 Ireland

6.2.2.2.1 DPC - Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing (December 2021; see Chapter 5: Age of digital consent and age verification)

Title	Fundamentals for a Child-Oriented Approach to Data Processing [i.12]
Organization	Data Protection Commission
Source (link, URL…)	https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf
Country	Ireland
Short description	
The "Fundamentals for a Child-Oriented Approach to Data Processing" outlines 14 key principles aimed at enhancing the protection of children's personal data. These principles are designed to ensure that online service providers prioritize the best interests of children in all aspects of data processing. Key highlights include: 1. Floor of Protection: Ensure a baseline level of protection for all users unless age verification is reliably conducted. 2. Clear-Cut Consent: Require that children's consent is informed, specific, and unambiguous. 3. Zero Interference: Legitimate interests will avoid negatively impacting children. 4. Know Your Audience: Implement child-specific protections for services likely accessed by children. 5. Information in Every Instance: Children should always be informed about how their data is processed. 6. Child-Oriented Transparency: Provide clear and age-appropriate privacy information. 7. Let Children Have Their Say: Recognize and respect children's rights over their data. 8. Consent Does not Change Childhood: Avoid treating children as adults based on their consent. 9. Your Platform, Your Responsibility: Ensure robust age and parental consent verification. 10. Do not Shut Out Child Users: Provide a rich service experience without bypassing obligations. 11. Minimum User Ages Are not an Excuse: Adhere to GDPR [i.4] obligations even with theoretical age thresholds. 12. Precautionary Approach to Profiling: Avoid profiling children for marketing unless it clearly benefits them. 13. Do a DPIA: Conduct Data Protection Impact Assessments with a focus on children's best interests. 14. Bake It In: Incorporate high-level data protection by design and default across all services processing children's data. These fundamentals aim to guide policymakers, implementers, and organizations in ensuring robust, child-centric data protection practices.	

Stakeholder	Requirements
Underage users of internet services and recipients of information groups.	• Ensure underage users benefit from a guaranteed baseline level of data protection and that their personal information is secure even when reliable age verification is not conducted. • Require informed, specific, and unambiguous consent so children are better equipped to understand what they are agreeing to. • Make sure that privacy information is clear and age-appropriate; provide information in a manner that children can understand, enhancing their comprehension of how their data is used and their rights regarding their personal information. • Ensure that data processing activities prioritize the best interests of children, and that legitimate interests do not negatively impact them. • Embed high-level data protection by design and default, ensuring that robust privacy measures are automatically in place when processing children's data. • Develop and implement protections specifically designed for child users, including creating child-friendly interfaces, providing age-appropriate content, and ensuring that the service environment is safe and supportive for minors. • Conduct regular DPIAs with a focus on children's best interests.
Parents of underage users.	• Ensure there is a baseline level of data protection, so parents gain confidence in online services. • Ensure that children's consent is informed, specific, and unambiguous, so parents can be more confident that their children are making knowledgeable decisions about their data. • Provide clear and age-appropriate privacy information, so parents can guide their children through understanding online privacy and data protection, fostering better digital literacy within the family. • Implement child-specific protections and a precautionary approach to profiling, to assure parents that their children are not being exploited for marketing or other commercial purposes. • Ensure robust age and parental consent verification mechanisms are in place, to support parents in their role of safeguarding their children's online presence.
Adult users of internet services and recipients of information groups.	• Ensure a baseline level of protection for all users, to raise data privacy standards across the board and allow adults to experience improved data security and privacy practices as a result of the child-oriented approach. • Refine and clarify consent practices for adult users, so they can benefit from a more transparent and understandable process for how their data is collected and used. • Ensure legitimate interests are not negatively impacting children as part of a more ethically responsible data processing environment. Adults, as part of this ecosystem, can then benefit from a culture of responsible and ethical data handling practices. • Incorporate high-level data protection standards by design and default for children to lead to improved overall design practices that benefit all users.
Providers of age verification services and national authorities providing age verification solutions.	• Ensure that the age verification process is thorough and accurate, aligning with the emphasis on protecting children's data. • Implement child-specific protections to comply with regulations that require services likely to be accessed by children to have such measures. • Develop and integrate innovative technologies that cater specifically to the nuances of verifying children's ages and protecting their data. • Adhere to high standards of transparency and privacy, ensuring that the age verification process does not compromise user data. • Work closely with online service providers to implement robust age and parental consent verification mechanisms. • Ensure that verification processes are seamlessly integrated into online services while maintaining compliance with data protection regulations. • Conduct regular DPIAs with a focus on children's best interests.
Service providers which need age information to ensure that minors receive only adequate information and services as defined/required by parents or by legal restrictions.	• Meet the baseline level of protection for all users, especially minors, by implementing robust age verification processes. • Establish clear, specific, and unambiguous consent mechanisms tailored to children, ensuring that minors and their parents understand what they are consenting to. • Offer clear, age-appropriate privacy information, to ensure that children are always informed about how their data is processed. • Conduct regular DPIAs with a focus on children's best interests.

6.2.2.3 Spain

6.2.2.3.1 AEPD - Decalogue of principles: Age verification and protection of minors from inappropriate content (December 2023)

Title	Decalogue of principles: Age verification and protection of minors from [i.13]
Organization	AEPD (Agencia Española de Protección de Datos) Spanish Data Protection National Authority
Source (link, URL…)	https://www.aepd.es/guias/decalogo-principios-verificacion-edad-proteccion-menores.pdf
Country/Region	Spain

Short description

The document "Decálogo de principios: Verificación de edad y protección de menores de edad ante contenidos inacuedos" by the Spanish Data Protection Agency (AEPD) outlines the key principles for verifying age and protecting minors from inappropriate content online. The document emphasizes the importance of ensuring that the age verification system is transparent, auditable, and adjustable, while also respecting the privacy and rights of all users; and highlights the need for a comprehensive approach to age verification and protection of minors, involving multiple stakeholders and ensuring that the system is designed to protect the interests of all users. The principles outlined in the document include:

1. Anonymity: Ensure that minors cannot be identified, tracked, or localized through the internet.
2. Verification of age: The verification of age is oriented towards ensuring that individuals with the appropriate age can access content, without allowing minors to be identified.
3. Limitation of access: The system limits access to content only when necessary, and not require individuals to define themselves as "authorized to access" in all situations.
4. No profiling: The system prevents profiling of individuals based on their navigation or activities.
5. Unlinkability: The system prevents the linking of an individual's activities across different services.
6. Parental authority: The system respects the authority of parents to educate their children and ensure that the protection of minors does not compromise their rights.
7. Transparency and accountability: The system is transparent and accountable, with clear guidelines for data processing and protection.
8. No discrimination: The system does not discriminate against individuals based on their age, race, or any other characteristic.
9. Protection of rights: The system protects the rights of all individuals, including their right to privacy and freedom of expression.
10. Governance: The system has a clear governance framework that ensures the protection of minors and the rights of all individuals.

Stakeholder	Requirements
Underage users of internet services and recipients of information groups.	• No profiling or tracking of minors. • No linking of activities across different services.
Parents of underage users.	• Confidence in the age verification system to ensure their children are protected. • Ability to adjust the system for minors with special needs.
Adult users of internet services and recipients of information groups.	• Confidence in the age verification system to ensure their children are protected. • Ability to adjust the system for minors with special needs.
Providers of age verification services and national authorities providing age verification solutions.	• Confidence in the age verification system to ensure their children are protected. • Ability to adjust the system for minors with special needs.
Service providers which need age information to ensure that minors receive only adequate information and services as defined/required by parents or by legal restrictions.	• Confidence in the age verification system to ensure their children are protected. • Ability to adjust the system for minors with special needs.

6.2.2.3.2 Draft Spanish law on the protection of children and adolescents in the digital environment

Title	Draft Spanish law on the protection of children and adolescents in the digital environment [i.14]
Organization	Spanish Government
Source (link, URL…)	Confidential. Distributed to the Spanish expert group.
Country/Region	Spain

Short description

This draft aims to ensure that children and adolescents are protected from harmful digital content and have access to safe and secure digital environments. It recognizes the rights of children and adolescents to be protected from digital content that may harm their development and to receive adequate information about the use of digital technologies.
The law includes various measures to achieve these goals, such as:

1. Obligations on manufacturers to provide information about the risks associated with their products and to include parental control features.
2. The creation of an Estrategia Nacional sobre la Protección de la Infancia y la Adolescencia en el Entorno Digital to promote digital literacy and safe use of digital technologies.
3. The inclusion of digital literacy and safety in the curriculum of educational institutions.
4. The establishment of a code of conduct for internet service providers to ensure safe access to the internet.
5. The creation of a system for reporting and addressing harmful digital content.

Specific measures for age verification and parental control
The draft includes specific measures for age verification and parental control:

1. Age Verification: The law requires manufacturers to include mechanisms for verifying the age of users, particularly in the case of video games and other digital products that may contain harmful content.
2. Parental Control: The law obliges manufacturers to include parental control features in their products, such as the ability to limit access to certain content or set time limits for use. These features will be activated by default during the initial configuration of the device and will be free for users.
3. Information Provision: Manufacturers will provide information about the risks associated with their products, including the potential for addiction and the impact on mental and physical health.
4. Verification of Compliance: Manufacturers will verify that their products comply with the law's requirements and conditions, and importers, distributors, and sellers will also verify compliance.
5. Regulatory Oversight: The Ministry for Digital Transformation and Public Function will oversee compliance with the law's requirements and conditions, including conducting inspections and imposing sanctions as necessary.

Use of the European Digital Identity Wallet (EUDI Wallet) The law will use the EUDI Wallet in the following cases:

1. The National Commission on Markets and Competition can request judicial authorization to order the cessation of activity of an adult video sharing platform that does not include age verification mechanisms aligned with the technical specifications of the EUDI Wallet, as per Regulation (EU) 2024/1183 [i.2].
2. Digital device manufacturers are expected to incorporate data protection and purpose limitation features that are at least equivalent to those of the EUDI Wallet, in accordance with Regulation (EU) 2024/1183 [i.2].

These measures aim to ensure that children and adolescents are protected from harmful digital content and have access to safe and secure digital environments.

Stakeholder	Requirements
Underage users of internet services and recipients of information groups.	• Age verification: Ensure that age verification mechanisms are in place to prevent access to harmful content and protect personal data. • Parental Control: Provide parental control features to limit access to certain content or set time limits for use. • Information provision: Receive information about the risks associated with internet use, including addiction and mental health impacts. • Data protection: Ensure that personal data is protected and not shared without consent. • Protection from harmful content: Prevent access to harmful content, such as messages and content with stereotypes of gender, discrimination, violence, or misinformation. • Access to safe online environments: Ensure that children have access to safe online environments that are free from harmful content and promote positive interactions. • Protection from health risks: Prevent access to content that promotes unhealthy habits, such as drug use, sex, or gambling. • Protection from economic risks: Prevent access to fraudulent or misleading content that can lead to financial losses. • Protection from social risks: Prevent access to content that promotes social isolation or negative interactions. • Protection from emotional risks: Prevent access to content that can cause emotional distress, such as violent or pornographic content. • Protection from cognitive risks: Prevent access to content that can negatively impact cognitive development, such as excessive screen time. • Protection of children's rights: Ensure that children's rights are respected and protected in digital environments, including the right to be protected from harmful content and the right to access information and services safely. • Support for digital literacy: Support the development of digital literacy skills in children, including the ability to use technology safely and responsibly.
Parents of underage users.	• Age verification: Ensure that age verification mechanisms are in place to prevent access to harmful content and protect personal data. • Parental control: Have parental control features available to limit access to certain content or set time limits for use. • Information provision: Receive information about the risks associated with internet use, including addiction and mental health impacts. • Data protection: Ensure that personal data is protected and not shared without consent. • Participation in policy design: Participate in the design, monitoring, and evaluation of policies that affect them directly. • Collaboration with authorities: Collaborate with authorities to ensure that measures are in place to protect children from online harms and to promote a safe and responsible use of technology.
Adult users of internet services and recipients of information groups.	• Anonymity.

Stakeholder	Requirements
Providers of age verification services and national authorities providing age verification solutions.	• Technical specifications: Comply with technical specifications for age verification mechanisms, including those outlined in the European Digital Identity Wallet (EUDI Wallet) Regulation (EU) 2024/1183 [i.2]. • Data protection: Ensure that personal data is protected and not shared without consent, with measures at least equivalent to those of the EUDI Wallet. • Regulatory compliance: Comply with regulatory requirements for age verification and data protection, including those outlined in the European Digital Identity Wallet (EUDI Wallet) Regulation (EU) 2024/1183 [i.2]. • Age verification mechanisms: Implement age verification mechanisms that are aligned with the technical specifications of the EUDI Wallet and that limit access to certain content or services based on age. • Parental consent: Obtain parental consent for minors to access certain content or services. • Information provision: Provide information about the risks associated with internet use, including addiction and mental health impacts. • Data protection: Ensure that personal data is protected and not shared without consent. • Technical support: Provide technical support for age verification mechanisms and ensure that they are compatible with different devices and platforms. • Continuous improvement: Continuously improve age verification mechanisms to ensure they remain effective and secure. • Collaboration with authorities: Collaborate with national authorities to ensure that age verification mechanisms are in line with regulatory requirements and that any issues or concerns are addressed promptly.
Service providers which need age information to ensure that minors receive only adequate information and services as defined/required by parents or by legal restrictions.	• Technical specifications: Comply with technical specifications for age verification mechanisms, including those outlined in the European Digital Identity Wallet (EUDI Wallet) Regulation (EU) 2024/1183 [i.2]. • Data protection: Ensure that personal data is protected and not shared without consent, with measures at least equivalent to those of the EUDI Wallet. • Regulatory compliance: Comply with regulatory requirements for age verification and data protection, including those outlined in the European Digital Identity Wallet (EUDI Wallet) Regulation (EU) 2024/1183 [i.2]. • Age verification mechanisms: Implement age verification mechanisms that are aligned with the technical specifications of the EUDI Wallet and that limit access to certain content or services based on age. • Parental consent: Obtain parental consent for minors to access certain content or services. • Information provision: Provide information about the risks associated with internet use, including addiction and mental health impacts. • Data protection: Ensure that personal data is protected and not shared without consent. • Technical support: Provide technical support for age verification mechanisms and ensure that they are compatible with different devices and platforms. • Continuous improvement: Continuously improve age verification mechanisms to ensure they remain effective and secure. • Collaboration with authorities: Collaborate with national authorities to ensure that age verification mechanisms are in line with regulatory requirements and that any issues or concerns are addressed promptly.

6.2.2.4 United Kingdom

6.2.2.4.1 ICO - Age assurance for the Children's code (January 2024)

Title	Age assurance for the Children's code [i.15]
Organization	Information Commissioner Office (ICO)
Source (link, URL…)	https://ico.org.uk/about-the-ico/what-we-do/information-commissioners-opinions/age-assurance-for-the-children-s-code/
Country	UK
Short description	
The Children's code is a statutory code of practice. It sets out how Internet Society Services (ISS) likely to be accessed by children should protect children's information rights online. It explains how age assurance can form part of an appropriate and proportionate approach to reducing or eliminating the personal information risks children face online and facilitate conformance with the Children's code. This opinion is aimed at ISS and age assurance providers to explain how they can use the technology in compliance with data protection law in a risk-based and proportionate way.	
Stakeholder	**Requirements**
Underage users of internet services and recipients of information groups.	
Parents of underage users.	
Adult users of internet services and recipients of information groups.	
Providers of age verification services and national authorities providing age verification solutions.	• Make sure it is fair. • Establish a lawful basis to process the information. • Be transparent about how information is used. • Not use information collected for the purpose of age assurance for any other incompatible purpose. • Collect the minimum information required for the process. • Make sure the method is accurate. • Not retain any information collected by the method for longer than is needed. • Make sure the method is secure. • Be accountable for your compliance with the law (e.g. by adopting relevant policies and procedures).
Service providers which need age information to ensure that minors receive only adequate information and services as defined/required by parents or by legal restrictions.	• Establish the age of your users to comply with the code; or • Apply all standards of the code to all users in a risk-based and proportionate way. • If the service is not appropriate for children access should be restricted.

6.2.2.4.2 Ofcom - Guidance on age assurance and other Part 5 duties for service providers publishing pornographic content on online services: Annex 2 (December 2023)

Title	Guidance on age assurance and other Part 5 duties for service providers publishing pornographic content on online services [i.9]
Organization	Ofcom
Source (link, URL…)	https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/272586-consultation-guidance-for-service-providers-publishing-pornographic-content/associated-documents/annex-2-guidance-for-service-providers-publishing-pornographic-content-online
Country	UK

Short description

This guidance is for service providers that display or publish pornographic content on their online services to help them comply with their regulatory duties under the Online Safety Act 2023 ('the Act'). These duties include a requirement for service providers to implement age assurance to ensure that children are not normally able to encounter pornographic content displayed or published on their service.

This document gives guidance on:

- assessing whether a service is in scope of the Part 5 duties;
- examples of kinds of age verification and age estimation that may be suitable for the purposes of compliance, and criteria that service providers should fulfil to ensure the age assurance implemented is highly effective at correctly determining whether or not a particular user is a child;
- how service providers can keep a written record and produce a publicly available statement setting out how they have complied with their duties, including how providers may have regard to the importance of protecting users from breaches of privacy law in their written record; and
- the principles to be applied for compliance.

Stakeholder	Requirements
Underage users of internet services and recipients of information groups.	
Parents of underage users.	
Adult users of internet services and recipients of information groups.	
Providers of age verification services and national authorities providing age verification solutions.	

Stakeholder	Requirements
Service providers which need age information to ensure that minors receive only adequate information and services as defined/required by parents or by legal restrictions.	• Implement age assurance, for example using one or more of the methods listed in the guidance. • Ensure that the age assurance process used is: (a) of a kind that could be highly effective at correctly determining whether or not a user is a child; and (b) used in such a way that it is highly effective at correctly determining whether or not a user is a child. • Ensure that, by using the age assurance process in question, children are not normally able to encounter regulated provider pornographic content on the service (i.e. by using an effective access control measure). • Keep an easily understandable written record of: – the kinds of age assurance used and how they are used by the service provider or a third-party age assurance provider; – how the service provider has had regard to privacy and data protection laws when deciding which age assurance process to use and how. • Produce a publicly available summary of the parts of the written record relating to implementing highly effective age assurance, including the age assurance method(s) the service provider is using and how. • Ensure the age assurance process implemented fulfils the criteria of technical accuracy, robustness, reliability and fairness. • Consider the principles of accessibility and interoperability when implementing age assurance. • Implement any techniques to mitigate against attempts at circumvention of the age assurance process that are easily accessible to children and where it is reasonable to assume that children may use them. • Consider whether to offer alternative methods where an age assurance method is only highly effective for a limited number of users. • Ensure that the written record is durable, accessible, and up to date. • Familiarize themselves with the data protection legislation, and how to apply it to their age assurance method(s), by consulting guidance from the Information Commissioner's Office (ICO). • Refrain from hosting, sharing or permitting content that directs or encourages child users to circumvent the age assurance process or access controls.

6.2.3 Standards and Certifications

6.2.3.1 BSI PAS 1296:2018 - Online age checking. Provision and use of online age check services. Code of Practice (March 2018)

Title	BSI PAS 1296:2018 [i.16] Online age checking. Provision and use of online age check services. Code of Practice
Organization	British Standards Institute
Source (link, URL…)	https://knowledge.bsigroup.com/products/online-age-checking-provision-and-use-of-online-age-check-services-code-of-practice?version=standard
Country	UK
Short description	
Some businesses have a legal requirement to conduct online age checks: whether because they sell age-restricted merchandise (e.g. dangerous goods); stream adult content; or provide age-sensitive services such as dating or gambling. This PAS helps these businesses comply with regulation, and safeguard their reputation, by providing recommendations that help prove an online user's age. It can be used by: • Businesses mandated to conduct age checks • Businesses that want enhanced e-safeguarding - perhaps to differentiate themselves in their market • Age-checking services • Organizations with a legal, regulatory, supervisory, advisory or enforcement role around the deployment of age checking services by businesses • Consumer protection groups and consumers who can use the PAS as a resource It aims to protects consumers from age sensitive material, and it aims protects businesses by providing due diligence recommendations which help them make sure they are meeting specific regulatory compliance needs.	

Stakeholder	Requirements
Underage users of internet services and recipients of information groups.	
Parents of underage users.	
Adult users of internet services and recipients of information groups.	
Providers of age verification services and national authorities providing age verification solutions.	• Data minimization, for example a data controller limiting the collection of personal information to that which is directly relevant and necessary to accomplish a specified purpose. • Transparency and Consent. The GDPR [i.4] requires that valid consent is explicit for data collection and usage (see GDPR [i.4], Article 7; defined in Article 4). Moreover, data controllers are required to prove "consent" (opt-in), and consumers are required to be able to withdraw consent (Article 7; defined in Article 4). Consent for children below 13 or 16 years of age (the age threshold might differ in the member states) is required to be given by the child's parent or custodian and needs to be verifiable (Article 8). • Pseudonymization is an umbrella term for approaches like data masking that aim to protect confidential information that directly or indirectly reveals an individual's identity. Pseudonymization is a key concern of this PAS, which encourages the use of pseudonymization technologies. Article 4 of the GDPR [i.4] explains that pseudonymized data "can no longer be attributed to a specific data subject without the use of additional information", such as separately stored mapping tables. Where any such matching information exists, it is required to be kept separately and subject to controls that prevent it from being combined with the pseudonymized data for routine identification purposes. Data masking and hashing are examples of pseudonymization technologies.
Service providers which need age information to ensure that minors receive only adequate information and services as defined/required by parents or by legal restrictions.	

6.2.3.2 IEEE 2089-2021 - IEEE Standard for an Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children

Title	IEEE Standard for an Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children [i.17]
Organization	IEEE
Source (link, URL…)	https://xplorega.ieee.org/document/9627644
Country	USA

Short description

This standard is the first in a series focused on the 5Rights principles, establishing processes for creating age-appropriate digital services for children.
It focuses on:

- Recognizing users as children.
- Considering children's capacities and upholding their rights.
- Offering terms and presenting information appropriately for children.
- Providing validation for service design decisions.

It includes an impact rating system and evaluation criteria for vendors, public institutions, and educational sectors. The standard sets requirements for terms, design, and delivery to address children's needs and emphasizes compliance with legal and regulatory requirements for data privacy and security.
Purpose:
The purpose is to aid in tailoring digital services to be age-appropriate, enhancing safety, privacy, autonomy, and health for children. It provides guidelines and best practices, offering validation for design decisions.
Use of the Standard:
The standard outlines processes for engineers and technologists to consider children's rights and needs during concept exploration and development. It helps align innovation management with age-appropriate design and delivery, aiming to reduce risks and amplify digital benefits for users under 18. It reflects the 5Rights Foundation principles and the UN Convention on the Rights of the Child. Organizations should consider their engagement with children through data analytics, research, and surveys to apply this standard effectively.
Process Overview:
The goal is to design and deliver systems that prioritize children's rights and needs. Age appropriateness encompasses sustainability, privacy, usability, convenience, controllability, accountability, inclusivity, evolving capacity, and children's rights, alongside typical system engineering values like functionality, efficiency, and effectiveness.

Stakeholder	Requirements
Underage users of internet services and recipients of information groups.	• Implement features and controls that are suitable for children without requiring them to adjust settings or make informed decisions beyond their cognitive abilities. • When designing the service, consider the varying needs of children based on factors such as age, context, ethnicity, cognitive capacity, and socioeconomic status. • Create mechanisms by which a diverse range of children can be consulted directly or with the help of a third party. • Obtain valid, informed and meaningful consent that is transparent about the risks associated with the nature and features of a product or service. • Publish terns that are inclusive to the evolving capacity and inclusive of all children and young people. • Apply privacy preserving age assurance mechanisms proportionate to the risk and nature of the product or service. • Provide options for children to retract, correct, and delete their data, consistent with applicable laws and regulations; do this in a way that is accessible and transparent. • Provide children access to expert advice and support where needed.
Parents of underage users.	• Create mechanisms by which a diverse range of parents can be consulted directly or with the help of a third party. • Obtain valid and meaningful consent from parents or a responsible adult, consistent with all applicable laws and regulations. • Where children's data is shared with parents, accompany it with age-appropriate information that helps explain what data or activities are being shared. • Provide parents access to expert advice and support where needed.
Adult users of internet services and recipients of information groups.	• When designing the system, avoid unfairly favouring or excluding users based on geographic areas, biometric or demographic characteristics, or unvalidated reports. • Apply privacy preserving age assurance mechanisms proportionate to the risk and nature of the product or service.

Stakeholder	Requirements
Providers of age verification services and national authorities providing age verification solutions.	• When designing the system, avoid unfairly favouring or excluding users based on geographic areas, biometric or demographic characteristics, or unvalidated reports. • Apply privacy preserving age assurance mechanisms proportionate to the risk and nature of the product or service. • Develop robust methods to accurately recognize users who are children. • Follow specific design guidelines outlined in the standard to ensure the systems are age appropriate.
Service providers which need age information to ensure that minors receive only adequate information and services as defined/required by parents or by legal restrictions.	• Apply privacy preserving age assurance mechanisms proportionate to the risk and nature of the product or service.

6.2.3.3 IEEE 2089.1-2024 - IEEE Draft Standard for Online Age Verification

Title	IEEE Standard for Online Age Verification [i.18]
Organization	IEEE
Source (link, URL…)	https://xploreqa.ieee.org/document/10542699
Country	USA
Short description	

IEEE 2089.1-2024 [i.18], provides a structured approach to designing, evaluating, and deploying age verification systems within digital services. Here are the key points outlined in the document:

Scope and Definitions:

- Establishes a framework for age assurance systems, covering age verification and estimation methods.
- Defines roles and responsibilities in the age assurance process.
- Specifies requirements for different confidence levels (asserted, standard, enhanced, strict) in age assurance.
- Emphasizes privacy protection, data security, and information system management tailored to age assurance.

Purpose:

- Aims to verify or estimate user age accurately and proportionally within digital services.
- Focuses on ensuring children's rights and needs are met, promoting safety, privacy, autonomy, and health.
- Provides guidelines and best practices for age assurance decisions, whether mandated by law or adopted voluntarily.

Word Usage:

- Clarifies terminology such as 'shall' for mandatory requirements, 'should' for recommendations, 'may' for permissible actions, and 'can' for capabilities within the standard.

Use of the Standard:

- Describes processes for leaders, managers, engineers, and technologists to implement age assurance.
- Lists minimum requirements for age assurance systems, including privacy protection, proportionality, security, accessibility, and effectiveness.
- Aligns with data protection legislation and the UN Convention on the Rights of the Child.

Implementation and Impact:

- Supports age-appropriate design in digital services, aligning with the 5Rights Foundation's principles.
- Encourages organizations to assess and implement age assurance systems where necessary, addressing risks to children effectively.
- Recognizes the complexity of data privacy and security laws, emphasizing compliance with evolving regulations.

Process Overview:

- Outlines sequential phases for age assurance: Determination, Selection, Assurance, and Categorization.
- Emphasizes continuous practices of Privacy, Data Security, and Interoperability throughout the age assurance lifecycle.

Overall, IEEE 2089.1-2024 [i.18] aims to enhance the safety and inclusivity of digital environments for children, ensuring compliance with legal standards while promoting best practices in age verification and estimation systems.

Stakeholder	Requirements
Underage users of internet services and recipients of information groups.	• Design systems that accommodate differences in children (age, ethnicity, socioeconomic background) by offering varying levels of support and consideration, such as accessibility features for different abilities or languages. • Build digital services that are suitable for children of different ages, considering developmental stages, cognitive abilities, and comprehension levels. • Provide children with clear information about their rights, the nature of the service, and how their data will be used. • Ensure that age assurance systems provide differentiated access to services and products, based on the age of the child user. • Confirm that each of the selected methods of age assurance offer functionality appropriate to the capacity and age of a child who might use the service. • Allow children full access to services which they should reasonably have access, e.g. news, health and education services, in line with the UN Convention on the Rights of the Child.
Parents of underage users.	• Acknowledge that not all children have actively engaged or capable parents or guardians and do not assume parental oversight and literacy in digital matters. • Design systems that do not rely solely on parental consent or guidance.
Adult users of internet services and recipients of information groups.	• Maintain the privacy of user data, as well as the security, accuracy and integrity of the age assurance process. • Confirm that each of the selected methods of age assurance are proportionate, having regard to the risks arising from the product or service and to the purpose of the age assurance system. • Confirm that each of the selected methods of age assurance are effective in verifying the actual age or age range of a user as required. • Confirm that each of the selected methods of age assurance are secure and do not expose users or their data to unauthorized disclosure or security breaches.
Providers of age verification services and national authorities providing age verification solutions.	• Ensure that age checking is not synonymous with age appropriateness in design. • Ensure compliance with child rights principles and ethical standards in age assurance practices. • Adopt a child rights approach to age assurance, which not only verifies age but also considers the developmental needs and capacities of child users. • Maintain the privacy of user data, as well as the security, accuracy and integrity of the age assurance process.
Service providers which need age information to ensure that minors receive only adequate information and services as defined/required by parents or by legal restrictions.	• Ensure compliance with child rights principles and ethical standards in age assurance practices. • Maintain the independence of the age assurance process from other aspects of its management, systems, and operations. • Determine and document the need for age assurance, of all or specific elements of the service; including the age or age ranges and the reasons for action, including regulatory or corporate social responsibility.

6.2.3.4 Age Check Certification Scheme

Title	Technical Requirements for Data Protection and Privacy [i.36]
Organization	The Age Check Certification Scheme
Source (link, URL…)	https://ico.org.uk/media/for-organisations/documents/2620426/accs-2-2021-technical-requirements-aadc.pdf
Country	UK
Short description	
The document outlines detailed technical requirements for organizations involved in age verification services, focusing on the processing of personal data throughout its lifecycle. Key aspects covered include: • Development and implementation of age check policies, including data deletion and anonymization. • Secure handling of data creation, storage, usage, archival, and destruction. • Implementation of robust data privacy, protection, and security measures, including vulnerability scanning and penetration testing. • Ensuring compliance with data subject rights such as access, rectification, erasure, and data portability. • Management of automated decision-making and profiling of personal data. • Roles of Data Protection Officers and preparation of Data Protection Impact Assessments. • Requirements for subcontracting processing activities and handling age attributes. • Different types of age check services covered, such as Proof-of-Age ID Providers, Age Check Providers, Age Check Exchange Providers, and Relying Parties. • Specific data processing activities encompassed, including age attributes, biometric attributes, personal identifiable information, customer records, authentication tokens, special category data, profiling, pseudonymisation, consent management, and cross-border data processing. The Age Certification Scheme is a UKAS accredited body and approved by the Information Commissioner's Office under UK GDPR [i.4] regulations. It mandates adherence to international, national, and local standards, emphasizing data protection enhancements and clarity in communication with children.	
Stakeholder	**Requirements**
Underage users of internet services and recipients of information groups.	• In terms of consent management, provide age-appropriate information for online services offered directly to children. • Separate requests for consent from terms and conditions, always using plain language.
Parents of underage users.	• In terms of consent management, obtain parental consent for children under 13 years of age.
Adult users of internet services and recipients of information groups.	• Make it easy to withdraw consent without any negative consequences. • Ensure consent is granular and allows individuals to consent separately to different types of processing. • Enable users to make informed decisions by providing transparent privacy information.
Providers of age verification services and national authorities providing age verification solutions.	• Identify and document the lawful basis for each processing activity involving personal data. • Only collect and process personal data that is adequate, relevant and necessary for the purposes for which they are processed.
Service providers which need age information to ensure that minors receive only adequate information and services as defined/required by parents or by legal restrictions.	• Integrate data protection considerations into every stage of service and product development. • Document risks, involve Data Protection Officers (DPOs), incorporate feedback from stakeholders and staff, and maintain records for at least 12 months post-launch to ensure ongoing compliance and improvement.

6.2.3.5 NIST - Face Analysis Technology Evaluation (FATE) Age Estimation & Verification

Title	Face Analysis Technology Evaluation: Age Estimation and Verification [i.19]
Organization	NIST
Source (link, URL…)	https://pages.nist.gov/frvt/html/frvt_age_estimation.html https://pages.nist.gov/frvt/reports/aev/fate_aev_report.pdf
Country	USA

Short description

The document explains that the motivation behind the report stems from recent legislation inside and outside the US driving the need for reliable age assurance methods to verify if individuals are above certain ages (e.g. 18, 21) for various purposes, such as alcohol sales or online access. Software-based face analysis is a potential approach using ubiquitous, inexpensive cameras. This method can function without storing photos or biometric data.

Overview:

Age assurance applications utilize either:

- Age Verification (AV) algorithms, which provide a yes/no answer to whether someone is above a certain age.
- Age Estimation (AE) algorithms, which produce a numeric age estimate.

The report evaluates six AE and AV software prototypes using around eleven million photos from four sources: immigration visas, arrest mugshots, border crossings, and immigration office photos. The report presents age estimation accuracy globally and by demographic group, explores performance in age verification tasks, and examines the impact of image quality. It does not include performance in interactive sessions, effects of disguises or cosmetics, nor does it address policy or recommend AV thresholds.

Audience:

The report is intended for:

- Actual and prospective deployers of AE technology.
- Policymakers assessing the technology's capabilities for specific use-cases.
- Developers, by highlighting factors affecting performance and comparing different prototypes.

Results:

- Age estimation accuracy has improved since 2014.
- Accuracy varies significantly based on the algorithm, sex, image quality, region-of-birth, age, and interactions among these factors.
- No single algorithm is superior across all metrics and demographics.
- Developers are expected to enhance capabilities over time.
- Future reports will focus on online safety for young teenagers, new datasets, and extended analyses.

Stakeholder	Requirements
Underage users of internet services and recipients of information groups.	• Implement additional age assurance measures for users estimated to be below a certain age threshold (Challenge-T). This can include secondary verification steps like government-issued ID checks or parental consent.
Parents of underage users.	• Implement additional age assurance measures for users estimated to be below a certain age threshold (Challenge-T). This can include secondary verification steps like government-issued ID checks or parental consent.
Adult users of internet services and recipients of information groups.	• Given that False Positive Rates (FPR) decrease with higher Challenge-T values, take a balanced approach to minimize the inconvenience for of-age users. • Implement a multi-level age verification process, especially for age-restricted applications and services. This includes a Challenge-T policy that adds additional verification steps when users are estimated to be below a certain age threshold.
Providers of age verification services and national authorities providing age verification solutions.	• Implement robust age verification systems using the most accurate age estimation algorithms. • Regularly update and make improvements as new research continually enhances algorithm performance. • Ensure images submitted for verification follow standardized photographic deadlines, including having consistent high-quality images, head orientation and no obstructions like eye glasses. • Calibrate age verification systems to account for variations in error rates across different demographics (sex, ethnicity, etc.). • Establish a continuous monitoring system to assess the performance of age estimation algorithms in real time.
Service providers which need age information to ensure that minors receive only adequate information and services as defined/required by parents or by legal restrictions.	• Ensure compliance with age verification standards through regular reporting and analysis; be transparent in your reporting.

6.2.4 Age Assurance Projects

6.2.4.1 CNIL (France) - Demonstration of a privacy-preserving age verification process (June 2022)

Title	Demonstration of a privacy-preserving age verification process [i.20]
Organization	CNIL
Source (link, URL…)	https://linc.cnil.fr/demonstration-privacy-preserving-age-verification-process
Country	France
Short description	
The text discusses a new possible implementation of an age-verification system that allows users to prove they are over the legal age of majority without disclosing their actual age or identity. This system addresses the need for privacy-preserving age verification on restricted websites, such as those with adult content. Key Points: Privacy-Preserving Age Verification: • The system allows users to verify their age without revealing personal data. • This method prevents both the third-party verifier and the requesting site from identifying the user or the site involved in the verification. Two Main Processes: • Creating age information by a trusted entity. • Transmitting this age-verification to a service requesting it. Cryptographic Techniques: • Utilizes "group signatures" and "zero-knowledge proofs" to ensure anonymity and data minimization. • These methods allow a user to prove a statement (e.g. being over 18) without revealing additional information. Demonstrator Implementation: • An open-source demonstrator available on platforms like GitHub and Docker. • Simulates interactions between a website, a certified age-verification site, and a certifying authority. • Ensures the verification process meets privacy and security standards. System Functionality: • Websites require users to submit a signed challenge from a certified verifier. • The challenge confirms the user meets the age requirement without revealing their identity. • Certified third-parties can be audited and have their certification revoked if they fail to meet standards. Potential Improvements: • Enhance security measures and threat identification. • Implement more nuanced age thresholds to obscure the verification purpose. • Ensure user control over their data exchanges, potentially through automated mechanisms.	
Stakeholder	**Requirements**
Underage users of internet services and recipients of information groups.	• Design the system to comply with varying age thresholds for different legal requirements (e.g. 13, 15, 16…)
Parents of underage users.	
Adult users of internet services and recipients of information groups.	• Utilize advanced cryptographic methods, specifically group signatures and zero-knowledge proofs, to allow users to prove their age without revealing any other personal information. • Ensure that users have control over their data exchanges. • Implement a system that allows users to manage their age verification tokens securely on their devices and use automated token exchange mechanisms to simplify the process.
Providers of age verification services and national authorities providing age verification solutions.	• Implement a privacy-preserving system, where a third-party verifier conducts the age verification process without revealing the user's identity or the identity of the website requesting the information. • Utilize advanced cryptographic methods, specifically group signatures and zero-knowledge proofs, to allow users to prove their age without revealing any other personal information. • Design the system to comply with varying age thresholds and different use cases beyond just age verification for website access.
Service providers which need age information to ensure that minors receive only adequate information and services as defined/required by parents or by legal restrictions.	• Design the system to comply with varying age thresholds and different use cases beyond just age verification for website access. • Implement a privacy-preserving system, where a third-party verifier conducts the age verification process without revealing the user's identity or the identity of the website requesting the information.

6.2.4.2 AEPD (Spain) - Technical note - Description of the proofs on concept for systems for age verification and protection of minors from inappropriate content (December 2023)

Title	Technical note - Description of the proofs on concept for systems for age verification and protection of minors from inappropriate content (*Nota técnica: Descripción de las pruebas de concepto sobre sistemas de verificación de edad y protección de personas menores ante contenidos inadecuados)* [i.21]
Organization	AEPD (Agencia Española de Protección de Datos) Spanish Data Protection National Authority
Source (link, URL…)	https://www.aepd.es/guias/nota-pruebas-concepto-verificacion-edad.pdf
Country/Region	Spain
Short description	
The document from the Spanish Data Protection Agency (AEPD) outlines the concept tests for verifying age and protecting minors from inappropriate content online. The tests aim to demonstrate that it is possible to implement a system that complies with the principles of the General Data Protection Regulation (GDPR [i.4]) and ensures the protection of minors' rights while also respecting the privacy of all users. The tests involve two applications: one for accessing content and another for verifying age. The age verification application uses QR codes, digital identities stored in electronic wallets, or physical identity documents to ensure that the user's identity remains anonymous. The system is designed to prevent the identification, tracking, and profiling of minors online. The tests are conducted on various devices, including computers and video game consoles, and involve the following steps: • The user requests access to content labelled as suitable for adults only. • The content is blocked by the system, and the user is prompted to verify their age using the age verification application. • The user scans a QR code on their mobile device, which is read by the age verification application. • If the user is deemed old enough to access the content, the system grants permission, and the content is displayed without any restrictions. The tests demonstrate that it is possible to implement a system that protects minors without compromising the privacy of all users. The system is designed to be transparent, auditable, and adjustable by parents for minors with special needs. The document highlights the importance of ensuring that the system does not discriminate against users and that it respects the principles of the GDPR [i.4]. The tests also emphasize the need for confidence in the system among users, as any lack of confidence could lead to discrimination, self-censorship, and rejection of the system. Overall, the document provides a comprehensive overview of the concept tests for verifying age and protecting minors online, highlighting the key principles and technical details of the system.	
Stakeholder	**Requirements**
Underage users of internet services and recipients of information groups.	• Ensure that the age verification system is transparent and does not compromise the privacy of minors. • Protect minors from being identified, tracked, and profiled online.
Parents of underage users.	• Have confidence in the age verification system to ensure their children are protected. • Be able to adjust the system for minors with special needs.
Adult users of internet services and recipients of information groups.	• Have confidence in the age verification system to ensure they are not restricted from accessing content. • Not be subjected to discrimination or profiling based on their age.
Providers of age verification services and national authorities providing age verification solutions.	• Ensure that the age verification system complies with the General Data Protection Regulation (GDPR [i.4]). • Implement a system that is transparent, auditable, and adjustable.
Service providers which need age information to ensure that minors receive only adequate information and services as defined/required by parents or by legal restrictions.	• Ensure that the age verification system does not compromise the privacy of all users. • Implement a system that respects the principles of the GDPR [i.4].

6.2.5 Resources - Government

6.2.5.1 Digital Regulation Cooperation Forum (UK) - Families' attitudes towards age assurance (October 2022)

Title	Families' attitudes towards age assurance [i.22]
Organization	Research commissioned by the ICO and Ofcom
Source (link, URL…)	https://assets.publishing.service.gov.uk/media/6343dd3f8fa8f52a5803e669/Ofcom_ICO_joint_research_-_age_assurance_report.pdf
Country	UK
Short description	
This research was commissioned by the ICO and Ofcom to explore parents' and children's attitudes towards potential age assurance methods and provide context for how current methods fit into families' daily behaviour. Age assurance refers to various methods used to estimate or establish a user's age, which can be used to provide an age-appropriate experience online as well as preventing children from accessing adult, harmful, or otherwise inappropriate material. The research included in-depth interviews with eighteen families, involving media diary tasks, and eight focus groups - four with parents of children of similar ages and four with children in age groups ranging from 13 to 17.	
Stakeholder	**Requirements**
Underage users of internet services and recipients of information groups.	• When discussing accessing social media, games and video sharing platforms, children tended to default to self-declaration, due to the perceived ease of circumvention and desire to be able to access these platforms.
Parents of underage users.	• Parents and children felt that hard identifiers such as a passport or driving licence were the most effective age assurance method and leaned towards these for traditionally age-restricted activities, such as gambling or accessing pornography, that they felt required "tougher measures". • Both parents and children had concerns about the amount of effort required to use methods such as hard identifiers and did not want to have to use age assurance methods repeatedly each time they accessed a platform. • Some parents and children raised concerns about the amount of data sharing required in order to age assure using behavioural profiling, hard identifiers, and facial image analysis, but felt that using a secure third-party could mitigate some of these risks. • Parents and children had doubts about how effective facial image analysis would be, and some felt uncomfortable with the idea of their faces being used in this way. • Behavioural profiling was unpopular due to perceived inaccuracy. Some had concerns about data privacy risks, which were not perceived to be "worth the risk" given the perception of low accuracy. • Parent / guardian confirmation was liked by parents as a method that gave them the most control and flexibility. However, some had concerns about how it could work in practice and the ease of circumventing it.
Adult users of internet services and recipients of information groups.	
Providers of age verification services and national authorities providing age verification solutions.	
Service providers which need age information to ensure that minors receive only adequate information and services as defined/required by parents or by legal restrictions.	

6.2.5.2 Measurement of Age Assurance Technologies (2022)

Title	Measurement of Age Assurance Technologies [i.23]
Organization	A Research Report for the Information Commissioner's Office (ICO)
Source (link, URL…)	https://ico.org.uk/media/about-the-ico/documents/4021822/measurement-of-age-assurance-technologies.pdf
Country	UK
Short description	
This research report sets out the approaches to the measurement of age assurance technologies. The report starts by defining age assurance and its various components (such as self-declaration, deployment of artificial intelligence, hard identifiers, digital identity services and other current or potentially emerging technical measures which could be deployed). The emerging consensus is that a simple approach to describing the levels of confidence achieved by different assurance components would assist service providers, relying parties and those that regulate them.	
Stakeholder	**Requirements**
Underage users of internet services and recipients of information groups.	
Parents of underage users.	
Adult users of internet services and recipients of information groups.	
Providers of age verification services and national authorities providing age verification solutions.	
Service providers which need age information to ensure that minors receive only adequate information and services as defined/required by parents or by legal restrictions.	
Others.	Measures should be applied for the efficacy to age assurance systems based upon whether the output is continuous (i.e. age estimation) or binary (i.e. age verification). For continuous age assurance, there should be conformity test reports. For binary age assurance, there should be conformity test reports. A need to identify the appropriate levels of tolerance for acceptable age assurance systems.

6.2.5.3 Measurement of Age Assurance Technologies - Part Two (August 2023)

Title	Measurement of Age Assurance Technologies Part 2 - Current and short-term capability of a range of Age Assurance measures
Organization	A Research Report for the Information Commissioner's Office (ICO) and the Office of Communications (OFCOM)
Source (link, URL…)	https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/age-assurance-research/
Country	UK
Short description	
This report is intended to provide an understanding of the practicability and feasibility of developing a methodology for measuring the effectiveness and/or accuracy of age assurance systems across different services. The ICO and Ofcom had asked for an exploration of various age assurance methods across various industries and providers, including combined approaches, alongside an assessment of current effectiveness and anticipated effectiveness over the next five years.	
Stakeholder	**Requirements**
Underage users of internet services and recipients of information groups.	
Parents of underage users.	
Adult users of internet services and recipients of information groups.	

Stakeholder	Requirements
Providers of age verification services and national authorities providing age verification solutions.	
Service providers which need age information to ensure that minors receive only adequate information and services as defined/required by parents or by legal restrictions.	
Others.	The research suggests that age assurance systems could effectively be assessed according to a stated age gate (i.e. '13', '16', '18') representing the principal age of interest to the relying parties for a particular use case. In other words, it is important that the focus is on the age, or indeed the age range, at which a technology is being evaluated. With the issue of accuracy of age assurance systems. A further question arises, however, as to how often the age check should be deployed (i.e. every time a user visits, or periodically or just once) and how often a prior age assurance check of a user should be re-authenticated. This should be based on an analysis of risks and could usefully be subject to further research. This should not be confused with the overall measure of accuracy of the system - they are two distinct factors for consideration.

6.2.5.4 Yoti Facial Age Estimation White Paper

Title	Yoti Facial Age Estimation White Paper [i.24]
Organization	Yoti
Source (link, URL…)	https://www.yoti.com/wp-content/uploads/2023/12/Yoti-Age-Estimation-White-Paper-December-2023.pdf
Country	UK
Short description	
Yoti has developed facial age estimation technology that accurately determines a person's age from a facial image, without needing physical documents or human intervention. This technology complies with GDPR [i.4] principles, ensuring privacy by design and minimal data usage, only facial images are required, which are immediately deleted after processing. The accuracy of Yoti's technology is robust across genders and skin tones. For ages 13 to 17, the True Positive Rate (TPR) for estimating under 25 is 99,91 %, with negligible bias observed across genders and skin tones. Similarly, for ages 6 to 12, the TPR for estimating under 13 is 96,99 %, demonstrating minimal bias within this age group as well. Yoti utilizes a neural network for facial age estimation, achieving a Mean Absolute Error (MAE) of 1,4 years for both 13 to 17 year olds and 6 to 12 year olds. This accuracy supports regulatory efforts to restrict access to age-sensitive goods and services. Yoti prioritizes fairness and accuracy, continually improving its algorithm to reduce biases, particularly for older age groups and various skin tones. They adhere to GDPR [i.4] guidelines for data collection and actively address demographic changes in their training data to maintain fairness. The technology has been independently tested and certified, confirming its security and effectiveness in preventing identity fraud. It supports compliance with Children's Codes and Age Appropriate Design Codes without processing special category data. Overall, Yoti's facial age estimation technology represents a secure, privacy-respecting solution that scales efficiently, performing over 593 million checks worldwide. Continuous enhancements ensure its accuracy and usability, underscoring Yoti's commitment to ethical responsibility and regulatory compliance in age verification technologies.	
Stakeholder	**Requirements**
Underage users of internet services and recipients of information groups.	• Prioritize privacy by design, by minimizing data collection, ensuring deletion of images after processing, and avoiding the processing of special category data related to children. • Work to mitigate biases in the facial age estimation algorithm, particularly concerning different skin tones and genders among children. • Ensure that the rights and dignity of children are protected throughout the age verification process.
Parents of underage users.	• Educate children and their guardians about how the facial age estimation technology works, its purpose, and the importance of consent. • Provide children and their guardians with a clear understanding on how they can exercise control over the use of the data.
Adult users of internet services and recipients of information groups.	• Obtain informed consent from users, particularly when using biometric facial image data. • Be transparent about how age data is collected, processed, and stored.

Stakeholder	Requirements
Providers of age verification services and national authorities providing age verification solutions.	• Prioritize privacy by design, by minimizing data collection, ensuring deletion of images after processing, and avoiding the processing of special category data related to children. • Seek independent testing and certification of age verification technologies, to validate their security and effectiveness. • Actively mitigate biases in age estimation technologies, particularly concerning different genders and skin tone. • Adhere to GDPR [i.4] principles and other relevant data protection regulations.
Service providers which need age information to ensure that minors receive only adequate information and services as defined/required by parents or by legal restrictions.	• Be transparent about how age data is collected, processed, and stored. • Adhere to GDPR [i.4] principles and other relevant data protection regulations.

6.2.6 Resources - Academia and Civil Society

6.2.6.1 5Rights Foundation - But how do they know it is a child? (October 2021)

Title	But how do they know it is a child? [i.25]
Organization	5 Rights Foundation
Source (link, URL…)	https://5rightsfoundation.com/resource/but-how-do-they-know-its-a-child/
Country	UK
Short description	
The document discusses the UK's upcoming Online Safety Bill and emphasizes the importance of enhancing age assurance measures as part of a comprehensive strategy to create a safer digital environment for children. It highlights several key points: • Age assurance is essential but not a complete solution for online child safety - it simply verifies a user's age. • There is a need for a variety of age assurance tools tailored to different situations, not one-size-fits-all solutions. • Many existing technical solutions are misused for excessive data collection. • Children should only provide necessary information to prove their age, minimizing data disclosure. • Service providers often hesitate to take responsibility for children once their age is known. • Making services age-appropriate often involves disabling intrusive features rather than new age assurance technologies. • Lack of common definitions, standards, and oversight undermines age assurance solutions. • Establishing statutory codes for age assurance can drive innovation and diversity in digital products and services for children. • Proposed standards for age assurance include privacy protection, proportionality, user-friendliness, security, accessibility, transparency, and respect for rights. • Effective age assurance needs to be flexible to adapt to various circumstances in the digital realm. Ultimately, the document advocates for a regulatory framework that instils confidence among stakeholders children, parents, and businesses facilitating innovation and redesign in technology to support safe digital experiences for children.	
Stakeholder	**Requirements**
Underage users of internet services and recipients of information groups.	• Design age verification processes to be straightforward and easy for children to understand and use. • Offer clear channels for children and their guardians to seek redress or challenge decisions relating to age verification. • Ensure that age verification is conducted in a manner that respects children's dignity, autonomy, and legal rights. • Implement age assurance methods that adhere to established standards which ensure proportionality, accessibility, and respect for children's rights.
Parents of underage users.	• Offer clear channels for children and their guardians to seek redress or challenge decisions relating to age verification.
Adult users of internet services and recipients of information groups.	• Minimize data collection and retention to what is strictly necessary to verify a user's age.

Stakeholder	Requirements
Providers of age verification services and national authorities providing age verification solutions.	• Design age verification processes to be straightforward and easy for children to understand and use. • Implement robust security measures to safeguard children's personal information against unauthorized access, breaches, and misuse. • Offer clear channels for children and their guardians to seek redress or challenge decisions relating to age verification. • Ensure that age verification is conducted in a manner that respects children's dignity, autonomy, and legal rights. • Minimize data collection and retention to what is strictly necessary to verify a user's age. • Implement age assurance methods that adhere to established standards which ensure proportionality, accessibility, and respect for children's rights.
Service providers which need age information to ensure that minors receive only adequate information and services as defined/required by parents or by legal restrictions.	

6.2.6.2 The Center for Growth and Opportunity - Keeping Kids Safe Online: How Should Policymakers Approach Age Verification? (June 2023)

Title	Keeping Kids Safe Online: How Should Policymakers Approach Age Verification? [i.26]
Organization	The Center for Growth and Opportunity, Utah State University
Source (link, URL…)	https://www.thecgo.org/wp-content/uploads/2023/06/Age-Assurance_03.pdf
Country	USA

Short description

As policymakers across the US consider new regulations meant to protect children online, they are increasingly confronting a central challenge: to protect children online, it is needed to know who is a child.
This document discusses the complexities and challenges of determining the age of internet users, highlighting the trade-offs of various age assurance methods, such as submitting government IDs or using AI-based facial age estimation, each with its own drawbacks and implications.
The paper outlines the growing concern with online child safety among regulators and reviews relevant legislation at the international, national, and state levels. It also elaborates on the inherent trade-offs of different age assurance approaches.
To address these challenges, the paper provides ten recommendations for US regulators, categorized into three areas: balance, specificity, and understanding.
Balance:

- Conduct cost-benefit analyses of legislation.
- Adopt a risk-based assurance approach.
- Offer tax breaks for small companies using trusted third-party vendors.

Specificity:

- Task NIST with releasing guidance on online risks.
- Institute a voluntary certification program for age assurance vendors.
- Specify privacy practices for age assurance.
- Expand FTC guidance on COPPA compliance.

Understanding:

- Facilitate research on assurance methods and technologies.
- Establish state or federal age assurance sandboxes.
- Assess the impacts of existing state models.
- Require certified vendors to share evaluation data.
- These recommendations aim to guide US policymakers in crafting effective online child safety regulations, with insights that may also be valuable for international lawmakers.

Stakeholder	Requirements
Underage users of internet services and recipients of information groups.	• Implement robust and accurate age assurance systems that can reliably distinguish between children and adults without being overly intrusive. • Promote education and awareness about online safety and age verification processes among children. • Ensure transparency in privacy policies and data handling practices related to age assurance systems.

Stakeholder	Requirements
Parents of underage users.	• Promote education and awareness about online safety and age verification processes among parents and guardians. • Ensure transparency in privacy policies and data handling practices related to age assurance systems.
Adult users of internet services and recipients of information groups.	• Implement robust and accurate age assurance systems that can reliably distinguish between children and adults without being overly intrusive. • Ensure that any data collected for age verification purposes is handled with strict privacy protections. • Design age verification systems to be accessible and inclusive, ensuring that all users, including those without access to government IDs or advanced technology, can be verified.
Providers of age verification services and national authorities providing age verification solutions.	• Design age verification systems that minimize the amount of personal data collected and ensure that this data is stored securely and used solely for the purpose of age verification. • Design age verification systems to be accessible and inclusive, ensuring that all users, including those without access to government IDs or advanced technology, can be verified. • Ensure compliance with stringent privacy standards and practices for collecting, storing, and handling personal data. • Adopt and develop risk-based assurance approaches tailored to different levels of online risk exposure. • Facilitate continuous research and development of new age assurance methods and technologies. • Task national institutes (like NIST) with releasing detailed guidance on age verification practices and online risks. • Implement a voluntary certification program and regular auditing processes for age assurance vendors.
Service providers which need age information to ensure that minors receive only adequate information and services as defined/required by parents or by legal restrictions.	• Maintain transparency in how age verification systems are implemented and ensure fairness in their application.

6.2.6.3 UNICEF - Digital Age Assurance Tools and Children's Rights Online across the Globe: A discussion paper (April 2021)

Title	Digital Age Assurance Tools and Children's Rights Online across the Globe: A Discussion Paper [i.27]
Organization	UNICEF
Source (link, URL…)	https://c-fam.org/wp-content/uploads/Digital-Age-Assurance-Tools-and-Childrens-Rights-Online-across-the-Globe.pdf
Country/Region	

Short description

The report addresses the current state and future considerations for age assurance systems used to protect children online.

Key points include:

- Immaturity of Age Assurance Systems: Experts indicate these systems are not fully mature, but they are gaining momentum globally and locally as a potential solution. The Australian eSafety Commissioner highlights the nascent nature of age verification and the need for holistic approaches to online safety.
- Research and Public Confidence: The UK VoCO study calls for further research on the impact of age assurance, particularly on how it may affect different groups of children, before large-scale implementation to prevent discrimination and assess tool effectiveness.
- Investment and Maturation: Significant investments in technology and governance are likely to make age assurance more viable soon. However, several questions and barriers remain, needing further discussion.

Proposed Principles for Development and Use:

- Proportionate Usage: Use age assurance only to mitigate recognized harms with the least intrusive methods.
- Transparency: Children should know how and when age assurance tools are used and the data sources involved.
- Access: Protect children's rights to information, participation, expression, privacy, and data protection. Provide remedies for incorrect age estimations and avoid unnecessary access restrictions.
- Inclusion: Ensure marginalized groups are not discriminated against or excluded.
- Technical Considerations: Carefully consider the sharing of electronic IDs and the emergence of a mature ecosystem.
- Governance: Establish clear rationales for age-gating and an international regulatory framework prioritizing children's rights, with oversight and enforcement mechanisms.

The report concludes by emphasizing the need for continued discussion, research, and development to create effective, inclusive, and rights-respecting age assurance systems.

Stakeholder	Requirements
Underage users of internet services and recipients of information groups.	• Ensure proportionate usage: only implement age assurance tools when there is clear evidence that they will effectively mitigate recognized harms to children. • Implement mechanisms for children to correct incorrect age estimations and allow them to appeal access denials, basing this on the principle that access should only be restricted when absolutely necessary to prevent harm, based on evidence. • Design age assurance systems to prevent discrimination against marginalized groups of children, including children with disabilities and children from minority ethnic or religious groups. • Ensure transparency when communicating with children about how and when age assurance tools are being utilized. • Prioritize children's rights with a clear, internationally consistency regulatory framework.
Parents of underage users.	• Ensure transparency when communicating with parents and guardians about how and when age assurance tools are being utilized. • Design age assurance systems to prevent discrimination against marginalized groups of adults, including ensuring that those with disabilities are not required to provide more or more sensitive data compared to others.
Adult users of internet services and recipients of information groups.	• Fully inform adult users about how age assurance tools are used, including when tools and active and what data sources are being used to verify their age.

Stakeholder	Requirements
Providers of age verification services and national authorities providing age verification solutions.	• Ensure proportionate usage: only implement age assurance tools when there is clear evidence that they will effectively mitigate recognized harms to children. • Implement mechanisms for children to correct incorrect age estimations and allow them to appeal access denials, basing this on the principle that access should only be restricted when absolutely necessary to prevent harm, based on evidence. • Design age assurance systems to prevent discrimination against marginalized groups of children, including children with disabilities and children from minority ethnic or religious groups. • Develop a clear, internationally consistent regulatory framework to guide the implementation of age assurance systems.
Service providers which need age information to ensure that minors receive only adequate information and services as defined/required by parents or by legal restrictions.	

6.2.6.4 Praesidio Safeguarding - Making age assurance work for everyone: inclusion considerations for age assurance and children

Title	Making age assurance work for everyone: inclusion considerations for age assurance and children [i.28]
Organization	Praesidio Safeguarding
Source (link, URL…)	https://assets.publishing.service.gov.uk/media/642572d160a35e000c0cb1ae/age_assurance_technologies_and_inclusion_considerations.pdf
Country	UK

Short description

The document explores various age assurance methods used by technology and social media companies to regulate children and young people's access online. It delves into their implications for inclusion and exclusion, particularly for vulnerable groups such as children in care, those with special educational needs, and those outside mainstream education. The study combines interviews with stakeholders from companies, regulatory bodies, policy makers, child safety groups, as well as directly with children and their caregivers.

Key Findings:
Diversity of Methods and Their Implications:
- The research identifies four main categories of age assurance methods: hard identifiers (like passports or credit cards), verified parental consent (using parental verification), behavioural data using AI (profiling user behaviour), and biometric data with AI (facial recognition).
- Each method presents inclusion and exclusion risks depending on the user's circumstances, highlighting the need for a flexible approach.

Challenges with Hard Identifiers:
- Methods relying on hard identifiers were found to be the least inclusive. Many children, especially those in care or with special needs, lacked suitable forms of ID or had concerns about privacy and security.

Verified Parental Consent:
- While some parents found this method suitable, concerns were raised about children's privacy and the lack of consistent parental figures for children in care, potentially hindering access.

Behavioural Data and AI:
- AI-based methods were generally perceived positively as they were seen as less intrusive and more inclusive for vulnerable groups. However, concerns exist about accuracy and privacy.

Biometric Data and AI:
- There was support for biometric methods, although concerns about racial biases in facial recognition technology were highlighted as a barrier to inclusion.

Wider Themes:
- Stakeholders differed in their views on age assurance: companies were concerned about user resistance and service quality, while parents and caregivers generally supported measures to enhance child safety online.
- Data privacy and security were paramount concerns, with trust in platforms contingent on transparent data handling practices.

Digital Exclusion Risks:
- Vulnerable children, including those in care, often rely on the internet for inclusion and connectivity. Age assurance methods need to consider these children's unique challenges to avoid further digital exclusion.

Overall, the research emphasizes the complexity of implementing age assurance technologies that balance safety with inclusion for all children and young people online. It advocates for a nuanced, multi-method approach to accommodate diverse user needs and backgrounds effectively.

Stakeholder	Requirements
Underage users of internet services and recipients of information groups.	• Implement a range of age verification methods that cater to children's diverse circumstances and backgrounds; this includes options beyond hard identifiers like passports. • Develop and utilize AI-based age assurance methods that are inclusive and respectful of privacy concerns. • Implement robust data privacy and security measures that prioritize transparency in how underage users' data is collected, stored and used. • Clearly communicate with children how their data is collected, stored, and used, and provide mechanisms for users to control and delete data as needed.
Parents of underage users.	• Provide multiple avenues for parental involvement in age verification processes. This could include not only verified parental consent through traditional means but also alternative methods that accommodate varying degrees of parental engagement and responsibility. • Provide clear information to caregivers about how their children's data will be handled and protected, addressing concerns that could deter trust and adoption of age assurance measures.

Stakeholder	Requirements
Adult users of internet services and recipients of information groups.	• Address and mitigate any potential biases that arise from biometric data, including racial biases in facial recognition technologies. • Implement robust data privacy and security protocols that prioritize transparency in how users' data is collected, stored and used.
Providers of age verification services and national authorities providing age verification solutions.	• Implement a range of age verification methods that cater to children's diverse circumstances and backgrounds; this includes options beyond hard identifiers like passports. • Address and mitigate any potential biases that arise from the use of biometric data, including racial biases in facial recognition technologies. • Utilize AI-based age verification methods that prioritize accuracy while respecting user privacy.
Service providers which need age information to ensure that minors receive only adequate information and services as defined/required by parents or by legal restrictions.	

6.2.7 Resources - Industry Think Tanks

6.2.7.1 The Age Verification Providers Association - Privacy; a foundational concept for age verification (March 2024)

Title	Privacy; a foundational concept for age verification [i.29]
Organization	The Age Verification Providers Association
Source (link, URL…)	https://avpassociation.com/thought-leadership/privacy-a-foundational-concept-for-age-verification/
Country	UK
Short description	
The text discusses key aspects of age verification online, emphasizing privacy protection and compliance with legal standards: • Privacy Protection: Age verification allows proving age online without revealing identity. Users verify their age with an independent third party, which confirms age without retaining personal data. The process ensures data deletion post-verification and uses strong security measures akin to banking or healthcare. • Legal Compliance: In Europe (under GDPR [i.4]) and various US states (under laws like CCPA), strict data minimization and privacy-by-design principles apply. Age verification services will delete personal data immediately after verification, backed by legal penalties for non-compliance. • Technological Safeguards: Measures include encryption and avoiding centralized databases to prevent data breaches. Innovations like zero-knowledge proofs and device based verification (e.g. smartphone apps) enhance privacy, ensuring neither the website nor verification provider knows the user's identity. • Industry Standards: International standards (e.g. IEEE 2089.2021 [i.17]) ensure rigorous testing and certification of age verification systems. Audits by government-approved bodies verify compliance with data security and privacy standards. • Combatting Risks: Measures against phishing include referrals from reputable sites, audits for providers, and interoperability checks to prevent fake sites from joining networks. Facial age estimation, using AI to estimate age without identifying individuals, is an alternative for users preferring convenience and privacy. • Philosophy of Age Verification: The industry aims for age-awareness rather than identity-awareness online, focusing on anonymity. Unlike offline scenarios (e.g. showing ID at a bar), online verification strictly proves age without unnecessary disclosure.	
Stakeholder	**Requirements**
Underage users of internet services and recipients of information groups.	• Ensure the age verification process collects only the minimum necessary data from underage users, strictly limiting this to what is essential for verifying age. • Provide clear and accessible information to underage users about how age verification works, what data is collected, how it is used, and the measures in place to protect their privacy. • Implement enhanced security measures specifically tailored to protect the data of underage users. • Utilize age verification methods that are suitable for underage users and comply with legal requirements.

Stakeholder	Requirements
Parents of underage users.	• Implement a robust mechanism to obtain parental consent for underage users where required by law or policy. • Design parental consent mechanisms with privacy in mind, ensuring that parental consent is obtained securely and any data related to parental consent is handled confidentially. • Provide clear and accessible information to parents about how age verification works, what data is collected, how it is used, and the measures in place to protect their children's privacy.
Adult users of internet services and recipients of information groups.	• Obtain explicit consent from users before collecting any personal data, ensuring data minimization, and implementing strong security measures to protect personal information.
Providers of age verification services and national authorities providing age verification solutions.	• Adhere to international standards such as IEEE 2089.1 [i.18] and ISO/IEC 27566 [i.6], to ensure the age verification systems undergo rigorous testing and certification by government-approved auditors. • Implement risk mitigation measures to combat risks such as phishing and unauthorized access to personal data. • Conduct audits of age verification systems and practices, ensuring interoperability checks to prevent fake websites from participating in age verification processes. • Incorporate privacy-by-design principles into the systems. • Ensure the age verification process collects only the minimum necessary data from users, strictly limiting this to what is essential for verifying age.
Service providers which need age information to ensure that minors receive only adequate information and services as defined/required by parents or by legal restrictions.	• Conduct audits of age verification systems and practices, ensuring interoperability checks to prevent fake websites from participating in age verification processes. • Adhere to international standards such as IEEE 2089.1 [i.18] and ISO/IEC 27566 [i.6], to ensure the age verification systems undergo rigorous testing and certification by government-approved auditors. • Ensure the age verification process collects only the minimum necessary data from users, strictly limiting this to what is essential for verifying age.

6.2.7.2 Centre for Information Policy Leadership - Age Assurance and Age Verification Tools: Takeaways from CIPL Roundtable (March 2023)

Title	Age Assurance and Age Verification Tools: Takeaways from CIPL Roundtable [i.30]
Organization	Centre for Information Policy Leadership (CIPL)
Source (link, URL…)	https://www.informationpolicycentre.com/cipl-blog/age-assurance-and-age-verification-tools-takeaways-from-cipl-roundtable
Country	

Short description

The document explains that CIPL hosted a roundtable in 2023 to discuss age assurance tools' role in creating a safe online environment for minors. The event was part of CIPL's Children's Data Privacy Project, focusing on compliance issues outlined in their policy paper.

Legal Background:

- Global initiatives and legislation increasingly require digital services to verify or assess the age of users, particularly children.
- Various regulations like US COPPA, EU GDPR [i.4], and UK Age Appropriate Design Code mandate safeguards for children online.

Key Takeaways:

- Contextual Methodology: The effectiveness of age assurance methods depends on the specific risks and benefits of each online platform or service.
- No One-Size-Fits-All: Multiple age assurance methodologies exist (e.g. self-declaration, AI-based, biometrics), each with unique strengths and privacy considerations.
- Risk Assessment Guidance: Organizations need clear criteria and risk taxonomy for assessing appropriate age assurance methods under diverse regulatory environments.
- Children's Behaviour: Children may misrepresent their age online due to various factors, necessitating age assurance tools that consider these behaviours.
- Complementary Measures: Age assurance should be part of a broader strategy that includes privacy by design, transparency, content moderation, and parental controls.

Regulatory Challenges and Collaboration:

- There is a need for regulatory convergence across jurisdictions to harmonize age assurance standards.
- Initiatives like the UK Digital Regulatory Enforcement Forum facilitate cross-regulatory discussions on children's online safety.

Development and Standards:

- Stakeholders are actively involved in developing best practices and standards for age verification and assurance.
- Bottom-up standards and certifications are essential for widespread adoption and effectiveness of age assurance tools.

In summary, the roundtable highlighted the complexity of age assurance in digital environments, emphasizing the need for flexible methodologies that balance effectiveness with privacy concerns. It also underscored the importance of regulatory alignment and ongoing stakeholder collaboration to enhance children's online safety globally.

Stakeholder	Requirements
Underage users of internet services and recipients of information groups.	• Integrate age assurance tools into a broader strategy that includes privacy by design and transparency principles, to ensure that children's data is protected and their online interactions are safe and secure. • Regularly monitor and adapt age assurance methods as necessary to respond to evolving technological advancements and behavioural patterns among children online. • Maintain transparent privacy policies that outline clearly how age-related data is being collected, used, and protected.
Parents of underage users.	• Make parental control and guidance readily available to support guardians in monitoring and guiding their children's online activities. • Collaborate on educational aimed at raising awareness among parents about online risks, age assurance tools, and best practices for supervising children's digital activities. • Establish accessible channels for parents to provide feedback and report concerns related to age assurance or their children's privacy. • Collaborate with regulatory bodies to involve parents in shaping policies and standards related to children's online safety.
Adult users of internet services and recipients of information groups.	• Regularly monitor and adapt age assurance methods as necessary to respond to evolving technological advancements and behavioural patterns among users online.

Stakeholder	Requirements
Providers of age verification services and national authorities providing age verification solutions.	• Actively promote educational resources and tools to inform minors about safe online practices and the importance of truthful age representation. • Implement age verification mechanisms compliant with global initiatives and local regulations such as COPPA, GDPR [i.4] and the Age Appropriate Design Code. • Regularly monitor and adapt age assurance methods as necessary to respond to evolving technological advancements and behavioural patterns among children alone.
Service providers which need age information to ensure that minors receive only adequate information and services as defined/required by parents or by legal restrictions.	• Actively promote educational resources and tools to inform minors about safe online practices and the importance of truthful age representation. • Collaborate with regulatory bodies to involve parents in shaping policies and standards related to children's online safety. • Maintain transparent privacy policies that outline clearly how age-related data is being collected, used, and protected.

6.2.7.3 Centre for Information Policy Leadership - A Multi-Stakeholder Dialogue on Age Assurance (March 2024)

Title	A Multi-Stakeholder Dialogue on Age Assurance [i.31]
Organization	CIPL / WeProtect Global Alliance
Source (link, URL…)	https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/key_takeaways_from_a_multi-stakeholder_dialogue_on_age_assurance.pdf
Country	Global

Short description

The document covers several critical points and discussions involving a diverse range of stakeholders on age assurance.
Here are the key discussion points:
Age Assurance Overview:

- Age assurance involves both verification (e.g. identity documents, parental consent) and estimation (e.g. behavioural analysis, AI facial recognition). It emphasizes that self-declaration is inadequate for high-risk services and should be a continuous process rather than a one-time check.

Balancing Safety and Privacy:

- Organizations are urged to balance digital safety with user privacy, integrating privacy by design principles and employing proactive risk assessment techniques like red teaming.

Regulatory Landscape:

- Global legal and regulatory fragmentation complicates compliance, particularly in child privacy and safety. Efforts such as the Digital Regulation Cooperation Forum aim to harmonize approaches. Regulators require organizations to demonstrate the effectiveness of age assurance measures.

Context-and-Risk-Based Approach:

- There is no universal solution; strategies will be tailored to specific risks and contexts. Risk assessments should weigh both the likelihood and severity of harm, ensuring proportionate data collection.

Technical Challenges and Opportunities:

- Discussions include interoperability of age verification across platforms, adoption of privacy-enhancing technologies like zero-knowledge proofs, and the need for AI development in age assurance.

User Experience and Education:

- Tools for children, youth, and parents need to be accessible and understandable. Capacity-building among these groups is essential for effective use.

Ethical and Other Considerations:

- Equitable age assurance solutions are advocated, respecting privacy, security, and rights-based frameworks. Adaptation for diverse socio-economic, cultural, and disability contexts is stressed.

Developmental Considerations:

- Calls to reconsider age thresholds beyond age 13 and to adapt approaches for varying definitions of "the child" globally underscore the need for flexibility.

Overall, the dialogue underscored the complexity of age assurance, urging collaborative efforts for robust, inclusive, and privacy-conscious solutions to safeguard children online.

Stakeholder	Requirements
Underage users of internet services and recipients of information groups.	• Conduct thorough risk assessments tailored to different online services and contexts where underage users may engage. • Develop user-friendly age assurance tools that are accessible and can be easily understood by children. • Provide children with guidance on how to use age assurance tools effectively to enhance their online safety. • Ensure that age assurance solutions adhere to privacy by design principles.

Stakeholder	Requirements
Parents of underage users.	• Develop user-friendly age assurance tools that are accessible and can be easily understood by parents and guardians. • Implement a robust age assurance process that combines multiple methods, for example, identity verification, parental consent, and facial recognition.
Adult users of internet services and recipients of information groups.	• Integrate privacy by design principles into all age assurance solutions. • Develop and integrate privacy-enhancing technologies and methodologies that minimize data collection and storage.
Providers of age verification services and national authorities providing age verification solutions.	• Ensure that age assurance solutions adhere to privacy by design principles. • Adopt a context-and-risk based approach to age assurance, tailored to the specific risks and services. • Implement a robust age assurance process that combines multiple methods, for example, identity verification, parental consent, and facial recognition. • Establish a process for continuous monitoring and improvement of age assurance measures. • Develop interoperable age verification systems that allow for seamless age verification across different platforms and services.
Service providers which need age information to ensure that minors receive only adequate information and services as defined/required by parents or by legal restrictions.	• Conduct thorough risk assessments tailored to different online services and contexts where underage users may engage. • Establish a process for continuous monitoring and improvement of age assurance measures.

6.2.7.4 Digital Trust & Safety Partnership - Age Assurance: Guiding Principles and Best Practices (September 2023)

Title	Age Assurance: Guiding Principles and Best Practices [i.32]
Organization	Digital Trust & Safety Partnership
Source (link, URL…)	https://dtspartnership.org/wp-content/uploads/2023/09/DTSP_Age-Assurance-Best-Practices.pdf
Country	USA
Short description	
The document explains that digital services aim to create safe, age-appropriate experiences using "age assurance" methods to determine users' ages. These methods include age verification via identity documents or parental consent, age estimation from user data or physical traits, and self-declaration by users. Each method has trade-offs, particularly between accuracy and privacy, and may not be feasible for smaller companies. There is no universal solution; different services choose methods based on their user base, service type, risk assessment, privacy expectations, and economic viability. The Digital Trust & Safety Partnership outlines five guiding principles for age assurance: • Identify and mitigate risks to youth to inform proportionate age assurance methods. • Balance user privacy and data protection during development, implementation, and assessment of age assurance. • Ensure inclusivity and accessibility for all users, regardless of age, socioeconomic status, race, or other characteristics. • Implement layered enforcement of age assurance methods. • Maintain transparency and periodically report on age assurance practices. Challenges in creating age-appropriate digital services include defining suitable content across diverse cultures, involving parents, and respecting privacy while determining age accurately. There is no universally agreed standard, though efforts to create one are ongoing. Age assurance impacts user privacy, access to information, and freedom in digital spaces, and varies based on the service's nature and target audience. The document explains that developing effective practices involves consulting various stakeholders, including youth, to address these complex issues.	

Stakeholder	Requirements
Underage users of internet services and recipients of information groups.	• Provide underage users with clear information on how their data will be used and stored, etc. • Implement strict privacy safeguards to protect underage users' personal information collected during age verification. • Ensure that age assurance methods are inclusive and accessible to all underage users, regardless of socioeconomic status, race, or other characteristics. • Engage children, their parents, educators, and child safety experts in the development and ongoing assessment of age assurance methods. • Design content and safety features tailored to different age groups; ensure underage users are exposed only to appropriate content.
Parents of underage users.	• Develop robust systems and mechanisms for obtaining and verifying parental consent for underage users. • Maintain transparency about age assurance practices by periodically reporting to the public and stakeholders, including parents and guardians. • Provide clear information about methods used, any changes to policies, and the effectiveness of these measures in protecting their children.
Adult users of internet services and recipients of information groups.	• Ensure that age assurance methods are inclusive and accessible to all users, regardless of socioeconomic status, race, or other characteristics.
Providers of age verification services and national authorities providing age verification solutions.	• Ensure that age assurance methods are inclusive and accessible to all underage users, regardless of socioeconomic status, race, or other characteristics. • Implement strict privacy safeguards to protect underage users' personal information collected during age verification.
Service providers which need age information to ensure that minors receive only adequate information and services as defined/required by parents or by legal restrictions.	• Maintain transparency about age assurance practices by periodically reporting to the public and stakeholders, including parents and guardians. • Use age assurance methods that are accurate and proportionate to the risks associated with the service.

6.2.7.5 euCONSENT / Simone van der Hof - Methods for Obtaining Parental Consent and Maintaining Children Rights (September 2021); Age assurance and age appropriate design: what is required? (November 2021)

Title	Methods for Obtaining Parental Consent and Maintaining Children Rights [i.33]
Organization	Leiden University
Source (link, URL…)	https://euconsent.eu/download/methods-for-obtaining-parental-consent-and-maintaining-children-rights/
Country	The Netherlands

Short description

The document evaluates existing methods for age verification and parental consent in children's apps and games, assessing their compliance with the GDPR [i.4], especially Article 8, data minimization, and privacy by design principles.

Key findings include:

- Prevalence of Self-Declaration: Most apps and games rely on self-declaration for age verification, allowing easy circumvention by children, making parental consent potentially unlawful and inadequate for protecting children's data.
- Parental Consent Mechanisms: When present, parental consent methods often depend on self-declaration, such as providing a parent's email without verification, which compromises the efficacy of these mechanisms. Some exceptions involve more secure but privacy-intrusive methods like official document submission.
- Inadequacy for High-Risk Data Processing: Self-declaration is insufficient for high-risk data processing. High-risk scenarios should involve more secure methods, as children's data processing, particularly for commercial purposes, necessitates robust protections.
- Specific vs. General Consent: Parental consent often lacks specificity, with general agreements to privacy policies instead of clear, purpose-specific consents. Effective privacy settings that allow specific consents and easy withdrawal are recommended.
- Privacy-Preserving Verification: Verification methods should adhere to privacy by design principles, minimizing data collection and avoiding sensitive data use. Ideally, verifications should occur on the user's device to prevent large, vulnerable central databases.
- Transparency and Children's Rights: Verification processes will be transparent and understandable to children, ensuring their rights are prioritized. Including children and parents in designing verification methods ensures their needs and expectations are met.
- Evolving Capacities and Inclusivity: Verification methods should consider children's developmental stages and be inclusive, ensuring no child or parent is excluded due to verification requirements.
- Support and Remedies: Effective, age-appropriate support systems should be in place for children to address grievances or seek help with verification methods.

The study underscores the importance of a child rights impact assessment to balance GDPR [i.4] compliance with children's rights, recommending continuous involvement of children and parents in the process.

Stakeholder	Requirements
Underage users of internet services and recipients of information groups.	• Implement age verification methods that go beyond self-declaration to prevent circumvention. • Classify the processing of children's data, especially for commercial purposes like targeted advertising or profiling, as high-risk. • Implement stricter verification processes for high-risk data processing. • Design verification methods that are transparent and easy for children to understand. • Communicate, in a child-friendly manner, information about what data is collected, how it is used, and the purpose of verification. • Inform children what their parents are able to see and control, concerning their accounts. • Tailor verification methods to accommodate children of different ages and developmental stages. • Ensure verification processes are accessible to children with disabilities and those from diverse backgrounds.
Parents of underage users.	• Develop parental consent mechanisms that require verification beyond self-declaration. • Ensure that parental consent is specific to particular data processing activities rather than general data processing. • Provide clear, purpose-specific consent options, granting parents the choice of whether to agree to or decline, individual data processing activities. • Offer consent mechanisms that make it easy for parents to withdraw consent at any time.

Stakeholder	Requirements
Adult users of internet services and recipients of information groups.	• Implement stricter verification processes for high-risk data processing. • Design verification methods that are transparent and easy for users to understand. • Implement age verification methods that go beyond self-declaration to prevent circumvention.
Providers of age verification services and national authorities providing age verification solutions.	• Implement age verification methods that go beyond self-declaration to prevent circumvention. • Implement verified parental consent mechanisms that include multi-factor authentication or other secure verification methods, such as government-issued ID checks or secure document uploads. • Identify high-risk data processing activities and apply more stringent verification methods in these scenarios.
Service providers which need age information to ensure that minors receive only adequate information and services as defined/required by parents or by legal restrictions.	• Identify high-risk data processing activities and apply more stringent verification methods in these scenarios. • Adhere to privacy by design principles, ensuring that verification methods minimize data collection and avoid the use of sensitive data.

Title	Age assurance and age appropriate design: what is required? [i.33]
Organization	London School of Economics/Leiden University
Source (link, URL…)	https://blogs.lse.ac.uk/parenting4digitalfuture/2021/11/17/age-assurance/
Country	UK/EU

Short description

The document explores age assurance methods and different requirements.
Key points include:
Legal Requirements for Age Assurance:

- Age assurance encompasses various methods to verify the age of online users, essential for protecting children's vulnerability. While no general mandate exists for age verification, EU and national laws necessitate age differentiation in specific contexts, particularly for harmful content (18+ content, gambling, alcohol, and tobacco). The EU and UK data protection laws emphasize higher child protection, implying the need to verify users' ages for compliance. Exceptions occur when digital services inherently consider higher child protection.

Suitability of Age Assurance Methods:

- Different age assurance methods' suitability hinges on legal stipulations and specific contexts. Legislation may prescribe or allow flexibility in methods, particularly in protecting children and vulnerable groups. Age verification is one tool among others for child safety, such as age ratings and parental controls. Age estimation, using AI to guess users' ages, faces reliability issues, leading to potential underage access to harmful content or unjust denial to adults. Thus, direct age verification is recommended for legal compliance and liability concerns.

Data Protection Implications:

- Age verification can be privacy-preserving, not necessarily involving personal data processing. Device-based verification methods avoid creating vulnerable central databases. However, AI-based age estimation raises privacy issues, potentially necessitating user consent. Data minimization and privacy by design are crucial, though not always followed, leading to questions about algorithm-based age appropriateness determination by platforms. A risk-based approach is vital, given children's high data processing risks, and current self-declaration methods are insufficiently secure.

Age Verification and Child Rights:

- Children's rights, as per the UN Convention, require age-appropriate and privacy-friendly verification methods. Methods need to be understandable to children, and transparent about data processing. Effective, proportionate methods respecting all children's rights should undergo Child Rights Impact Assessments, with ongoing adjustments based on practical use. Children and parents should be involved in designing verification methods, ensuring they are context-sensitive, inclusive, and non-discriminatory, with mechanisms for complaints and support.

Future Developments:

- Currently, no age assurance method fully meets all outlined requirements. Existing solutions are either unfit or overly invasive, disclosing unnecessary personal data. Future methods need to prioritize children's rights and privacy, addressing surveillance concerns and developing inclusive, secure verification technologies.

Stakeholder	Requirements
Underage users of internet services and recipients of information groups.	• Transparency and understandability of age assurance methods to children. • Design methods in a way that children can easily understand, aligning with their developmental stages and capacities. • Ensure verification methods are context-sensitive and inclusive, catering to all children, including those with physical or cognitive barriers. • Implement a Child Rights Impact Assessment (CRIA) to evaluate how age verification methods affect children's rights. • Actively involve children in the design and development of age verification methods. • Provide accessible mechanisms for children to make complaints and seek support if their interests or rights are not being upheld.
Parents of underage users.	• Actively involve parents in the design and development of age verification methods. • Inform parents about the purpose of data collection and their rights regarding consent.
Adult users of internet services and recipients of information groups.	• Develop age verification methods that prioritize privacy and ensure minimal personal data processing. • Implement robust security measures, such as regular security audits and compliance with data protection standards such as the GDPR [i.4], to protect age verification data from unauthorized access.
Providers of age verification services and national authorities providing age verification solutions.	• Adhere to relevant EU and national laws regarding tailoring specific online content and services for users of different ages. • Adopt a privacy-preserving approach that involves data minimization, using encryption for data transmission, and avoiding the creation of vulnerable central data bases that could compromise user privacy. • Implement clear consent mechanisms, particularly when AI-based methods or sensitive personal data are involved. • Implement robust security measures, such as regular security audits and compliance with data protection standards such as the GDPR [i.4], to protect age verification data from unauthorized access. • Regularly assess and improve age verification methods based on feedback, technological advancements, and regulatory changes.
Service providers which need age information to ensure that minors receive only adequate information and services as defined/required by parents or by legal restrictions.	• Implement clear consent mechanisms, particularly when AI-based methods or sensitive personal data are involved. • Adopt a privacy-preserving approach that involves data minimization, using encryption for data transmission, and avoiding the creation of vulnerable central data bases that could compromise user privacy.

6.2.7.6 Family Online Safety Institute - Making Sense of Age Assurance: Enabling Safer Online Experiences (November 2022)

Title	Making Sense of Age Assurance: Enabling Safer Online Experiences [i.34]
Organization	Family Online Safety Institute (FOSI) Conducted by Kantar
Source (link, URL…)	https://cdn.prod.website-files.com/5f47b99bcd1b0e76b7a78b88/636d13257232675672619f45_MAKING%20SENSE%20OF%20AGE%20ASSURANCE%20FULL%20REPORT%20-%20FOSI%202022_compressed.pdf
Country	USA

Short description

The document examines the awareness and attitudes of parents and children towards age assurance methods in the US, UK, and France. By comparing these perspectives, the study aims to understand cultural differences in technology use, parenting styles, and attitudes toward safety and privacy.
For age assurance solutions to be accepted, parents and children need to understand their purpose and benefits. Technology companies and third-party providers have developed methods ranging from age gating to age estimation, and it is crucial that these methods are communicated transparently to foster trust. Involving children in the development of processes and policies that impact their online safety is also vital. The document discusses the complexities of age assurance in ensuring children access age-appropriate content online, highlighting that no perfect method currently exists.
Key points include:
Education and Empowerment:

- Parents and children need clear information on the purpose, process, and benefits of age assurance to make informed decisions and support these efforts.

Children's Perspectives:

- It is crucial to incorporate children's viewpoints in designing and implementing age assurance methods, especially as they grow older and manage their digital lives.

Balancing Effectiveness and Privacy:

- Solutions need to strike a balance between effectiveness and invasiveness, ensuring both safety and privacy, while also being convenient, reliable, and transparent. Collaboration and Future Preparation:
- Government, industry, and other stakeholders should collaborate to address current challenges and set a long-term vision for age assurance, considering future technological developments.

Enthusiastic Participation:

- Achieving effective age assurance solutions requires active involvement from industry, government, policy community, and parents, focusing on education, transparency, and trust.

Stakeholder	Requirements
Underage users of internet services and recipients of information groups.	• Educate children on why age assurance is necessary, as well as on the benefits it brings. • Actively involve children in the design and implementation of age assurance methods. • Design solutions with a focus on the user experience of children, making them easy to use for different age groups.
Parents of underage users.	• Foster trust among parents, children and other stakeholders through continuous education about age assurance methods and their benefits. • Educate parents on why age assurance is necessary and the benefits it brings for their children.
Adult users of internet services and recipients of information groups.	• Include clear policies on data usage and privacy protections. • Develop solutions that effectively verify age without being overly invasive.
Providers of age verification services and national authorities providing age verification solutions.	• Be transparent about how your age verification methods work. • Develop solutions that effectively verify age without being overly invasive. • Build age assurance methods that seamlessly integrate into the user experience without causing significant disruptions or inconvenience. • Design solutions with a focus on the user experience of children, making them easy to use for different age groups. • Engage in educational campaigns to inform parents and children about age assurance, its importance, and how it works.
Service providers which need age information to ensure that minors receive only adequate information and services as defined/required by parents or by legal restrictions.	• Work closely with government bodies, industry partners, and regulatory authorities to ensure that age assurance methods comply with legal standards and are widely accepted.

6.2.7.7 Future of Privacy Forum - Unpacking Age Assurance: Technologies and Tradeoffs (June 2023)

Title	Unpacking Age Assurance: Technologies and Tradeoffs [i.35]
Organization	Future Privacy Forum
Source (link, URL…)	https://fpf.org/wp-content/uploads/2023/06/FPF_Age-Assurance_final_6.23.pdf
Country	

Short description

Age Assurance encompasses various methods to determine an individual's age or age range, with no single method suitable for all situations. The context determines the appropriate level of certainty needed, balancing privacy risks and potential barriers to legitimate content, which can have unequal impacts. Often, a layered approach using multiple methods is recommended.

Age Assurance Considerations

Goals:

- Facilitate parental consent.
- Restrict access to age-specific services or content.
- Verify an individual's exact age.
- Place individuals within specific age bands (e.g. 13-15).

Potential Harms to Minors:

- Exposure to age-restricted content or services.
- Contact with unknown individuals.

Choosing the Appropriate Method:

- Select methods proportional to the goals and risks.
- Consider legal obligations that may mandate specific methods.

Balancing Assurance with Privacy:

- Assess privacy risks and mitigations.
- Ensure the assurance goal justifies the privacy risks and impacts.

Common Methods

Declaration

Age Gate:

- Users state their birthdate without evidence; suitable for low-risk situations but easily bypassed by minors. Privacy risk is low if birthdates are not retained.

Estimation

Facial Characterization:

- Uses a facial image to estimate age without uniquely identifying the individual. Effective for broad age bands but not for narrow distinctions (e.g. 17 vs. 18).

Verification

Biometric & Government ID:

- Matches government-issued ID with a live photo or video. Appropriate for high-risk, regulated services. Using only government ID provides less assurance.

Parental Consent/Vouching:

- A verified parent declares the child's age. Higher assurance than age gates but may limit teen autonomy.

Risks of Age Assurance:

- Limiting legitimate access.
- Equity and unequal access issues.
- Loss of anonymity.
- Sensitive data collection.
- Limiting teen autonomy.
- Potential misuse of data.
- Ability to bypass the methods.

Risk Management Tools:

- Immediate deletion of ID data.
- Use of third-party processors.
- Data minimization.
- On-device processing.

Stakeholder	Requirements
Underage users of internet services and recipients of information groups.	• Prioritize data minimization and on-device processing to protect children's privacy. • Ensure age assurance methods are accessible and do not unfairly disadvantage any child based on their socioeconomic status or background.
Parents of underage users.	• Facilitate parental consent mechanisms, ensuring that parents can authorize their child's access to services. • Design systems where parents can authorize access without overly restricting the independence of teenagers.

Stakeholder	Requirements
Adult users of internet services and recipients of information groups.	• Address potential inequities and ensure that age assurance methods do not disproportionately limit access to legitimate content for certain groups. • Implement age assurance methods that are proportional to the goals and risks of the specific service.
Providers of age verification services and national authorities providing age verification solutions.	• Prioritize data minimization and on-device processing to protect children's privacy. • Ensure immediate deletion of ID data and consider using third-party processors to separate data processing and storage. • Implement age assurance methods that are proportional to the goals and risks of the specific service. • Address potential inequities and ensure that age assurance methods do not disproportionately limit access to legitimate content for certain groups. • Use a layered approach by combining multiple age assurance methods to enhance accuracy and reliability.
Service providers which need age information to ensure that minors receive only adequate information and services as defined/required by parents or by legal restrictions.	• Adhere to legal obligations and ethical standards, ensuring that the chosen age assurance methods comply with relevant laws and regulations. • Regularly assess and mitigate potential harms, such as exposure to age-restricted content or contact with unknown individuals, to protect minors effectively. • Implement age assurance methods that are proportional to the goals and risks of the specific service.

6.2.7.8 Age Check Certification Scheme: Global Age Assurance Standards Summit 2024

Title	Global Age Assurance Standards Summit 2024 - Compendium [i.36]
Organization	Age Check Certification Scheme
Source (link, URL…)	https://accscheme.com/wp-content/uploads/ACCS-GlobalSummit-Compendium-.pdf?srsltid=AfmBOoowaicB9zuw8N-3-Id1xTBvGbxRhN6HvU_nHLLbixZB3E1SjCbM
Country	UK
Short description	
The Global Age Assurance Standards Summit, held in Manchester from April 8th to 12th, 2024, aimed to tackle the challenge of protecting children from harmful online content. With over 200 sessions, 77 hours of video, and 40 slide decks, the summit gathered global stakeholders to address the urgent need for age-aware internet policies and solutions. The summit was crucially timed amidst significant developments in age assurance standards, including ISO/IEC 27566-1 [i.6] and IEEE 2089.1 [i.18], highlighting a pivotal moment in global standards development. Manchester, known for its prominence in technology and regulatory bodies like the Information Commissioner's Office and Ofcom, provided an ideal setting for discussions and collaborations. Key objectives included advancing international age assurance standards, engaging regulators, showcasing innovative age verification technologies, compiling comprehensive evidence and knowledge for practitioners, and publishing a summit communique to inform global efforts, notably the United Nations Convention on the Rights of the Child. The summit underscored the shift towards biometric verification methods and emphasized the importance of certified age assurance solutions and conformity assessments to enhance online safety effectively. It advocated for cohesive global standards to complement national regulations, promoting technology-neutral approaches for robust online safety measures worldwide. Overall, the summit facilitated international cooperation, technological advancement, and regulatory strengthening to create safer online environments for children and secure access controls for adults, marking a significant step towards a more responsible digital future.	
Stakeholder	**Requirements**
Underage users of internet services and recipients of information groups.	• Implement stringent ethical guidelines and legal safeguards to protect children's privacy and rights during the age verification process. • Launch global educational campaigns aimed at children, parents, and educators to raise awareness about online safety, digital literacy, and responsible internet use.
Parents of underage users.	• Launch global educational campaigns aimed at children, parents, and educators to raise awareness about online safety, digital literacy, and responsible internet use.
Adult users of internet services and recipients of information groups.	• Implement stringent measures to safeguard user privacy and protect personal data during age verification processes.

Stakeholder	Requirements
Providers of age verification services and national authorities providing age verification solutions.	• Implement stringent ethical guidelines and legal safeguards to protect children's privacy and rights during the age verification process. • Design age verification solutions that are accessible and user-friendly, considering diverse user demographics including children, adults, and individuals with disabilities. • Seek certification from recognized authorities to validate the effectiveness and compliance of the age verification solution. • Implement and adhere to international age assurance such as ISO/IEC 27566-1 [i.6] and IEEE 2089.1 [i.18].
Service providers which need age information to ensure that minors receive only adequate information and services as defined/required by parents or by legal restrictions.	• Implement stringent measures to safeguard user privacy and protect personal data during age verification processes.

6.2.8 Resources - European Union

6.2.8.1 Mapping age assurance typologies and requirements (April 2024)

Title	Mapping age assurance typologies and requirements
Organization	European Commission
Source (link, URL…)	https://digital-strategy.ec.europa.eu/en/library/research-report-mapping-age-assurance-typologies-and-requirements
Country	Europe
Short description	
This research was commissioned by the European Commission under the "Better Internet for Children+" (BIK+) strategy. The resulting report seeks to explore the various aspects of age assurance, which is considered one of the solutions towards creating a safe online experience for children while promoting their well-being and respecting their rights and best interests. It considers ten main methods of age assurance and their advantages and disadvantages, as well as ten key requirements of age assurance tools. At the outset, it is relevant to understand when and why age assurance is legally to be used in certain cases and - in the absence of such a legal requirement - when (and in what form) it may be an adequate tool for the online protection of children.	
Stakeholder	**Requirements**
Underage users of internet services and recipients of information groups.	• Ensure that the rights of children enshrined under the United Nations Convention on the Rights of the Child (UNCRC) and the Charter of Fundamental Rights of the European Union (CFREU) are upheld. • Age assurance should not be construed as a silver bullet for online child protection. Instead, it should be considered as one of the many tools to protect and further the experiences of children online.
Parents of underage users.	
Adult users of internet services and recipients of information groups.	

Stakeholder	Requirements
Providers of age verification services and national authorities providing age verification solutions.	• In situations where age assurance (or, in particular, age verification) is not legally mandated but can be employed as a duty of care to children or as a contractual obligation or a voluntary measure, it should still be implemented with due regard to the potential exclusionary effects of age assurance. • Certain requirements that ought to be present, while assessing the necessity of age assurance and determining the method of age assurance to be implemented. The present report discusses ten such requirements: 1. Proportionality; 2. Privacy; 3. Security; 4. Accuracy and effectiveness; 5. Functionality and ease of use; 6. Inclusivity and non-discrimination; 7. Furthering participation and access; 8. Transparency and accountability; 9. Notification, challenge, and redressal mechanisms; and 10. Hearing the views of children.
Service providers which need age information to ensure that minors receive only adequate information and services as defined/required by parents or by legal restrictions	• Age assurance is legally relevant in three ways: 1. when a minimum age is prescribed by law for buying products or using services that may harm children or for performing legal acts, both of which require age assurance for legal compliance; 2. when there is a duty of care to protect children which may require age assurance to be employed; and 3. when there is a contractual obligation to provide the products or services only to users of a certain minimum or maximum age. • Even where no legal or contractual stipulations exist, platforms may still undertake age assurance in certain circumstances out of their own volition. • Other solutions such as age-appropriate design, age ratings, parental control tools etc., may be more appropriate in certain situations. • The primary responsibility for ensuring appropriate age assurance will be on the digital service providers themselves. • Any further guidance for online platforms, to provide them with assistance in applying measures that can ensure a high level of privacy, safety and security for children, while respecting their fundamental freedoms, would be welcome
Others	• European standardization bodies could provide further clarity to age assurance providers on how to implement age assurance solutions in an appropriate manner. That includes the European standard for online age verification, as envisaged under the European Commission's Better Internet for Kids (BIK+) strategy, which will develop an interoperable approach to age verification across borders and sectors. • Standards should include consideration of the effects of age assurance on the digital ecosystem and, more specifically, on the effective enforcement of legislation, to ensure both adequate protection of, and age-appropriate design for, children, as well as the creation of a level playing field for companies.

6.2.8.2 Age assurance self-assessment tool for digital service providers (May 2024)

Title	BIK age assurance self-assessment tool for digital service providers
Organization	European Commission
Source (link, URL…)	https://better-internet-for-kids.europa.eu/en/news/new-launch-bik-age-assurance-self-assessment-tool-digital-service-providers
Country	Europe
Short description	
To support and expand the implementation of proportionate age assurance methods, the Better Internet for Kids initiative (BIK) has launched a self-assessment guide, comprising the BIK self-assessment tool and an associated questionnaire. These tools are aimed at helping digital service providers to critically evaluate how their digital services may intersect with the protection of children and young people online. They support digital service providers by providing them relevant questions and offering practical guidance for making decisions related to age assurance so that they can have a robust age assurance process in place.	
Stakeholder	**Requirements**
Underage users of internet services and recipients of information groups.	
Parents of underage users.	
Adult users of internet services and recipients of information groups.	
Providers of age verification services and national authorities providing age verification solutions.	
Stakeholder	**Requirements**
Service providers which need age information to ensure that minors receive only adequate information and services as defined/required by parents or by legal restrictions	• It is strongly advised that digital service providers complement this self-assessment tool along with other assessments, such as a Child Rights Impact Assessment (CRIA), Data Protection Impact Assessment (DPIA), and Fundamental Rights Impact Assessment (FRIA) for high-risk artificial intelligence (AI) systems, and with their own legal assessment of compliance with their various obligations in this context. • The nature of the digital service and its risks to online child safety are analysed. This preliminary assessment is then used to determine the likely requirement for age assurance. • If it is determined that age assurance should be implemented, the level of assurance required of the age assurance process is to be ascertained. • Identify the age assurance tool(s) that can be utilized by the digital service provider, which could provide the required level of assurance. This involves an analysis of the availability of age assurance tool(s), the various advantages and disadvantages associated with such tool(s) and so on. This step culminates in a holistic analysis of the age assurance process to be implemented proportionately given the identified age assurance tool(s). • Important factors to be considered while implementing age assurance are assessed include factors such as whether circumvention techniques are addressed, how transparency will be maintained concerning age assurance, and so on. • Monitoring the performance of age assurance processes and undertaking a periodic review of them. • Two cross-cutting aspects to be considered while implementing age assurance: first, hearing the views of children and other stakeholders, and second, ensuring legal compliance.
Others	

7 Stakeholders requirements

7.0 Overview

The protection of underage users on the internet is a critical concern for various stakeholders, including regulatory bodies, service providers, and parents. The requirements for safeguarding these young users encompass numerous aspects, from privacy and data protection to ensuring safe access to appropriate content. This clause consolidates and categorizes the requirements extracted from various authoritative sources identified in clause 6, aiming to provide a clear and comprehensive guide for implementing effective age verification and protection measures.

7.1 Underage users of internet services and recipients of information groups requirements

This clause outlines key requirements for underage users of internet services and recipients of information groups, based on guidelines and principles from documents identified in clause 6. The aim is to provide a holistic approach to age verification and the protection of minors online, ensuring that their digital interactions are both safe and enriching.

The following requirements have been identified:

a) Privacy and data protection:

- Minimize data collection: Age verification processes should collect only the minimum necessary data from underage users to achieve the intended purpose, thereby reducing the risk of data misuse ("Age Assurance and Age Verification Tools: Takeaways from CIPL Roundtable" [i.31]).

- Transparency: It is essential to provide clear and accessible information to underage users about how age verification works, what data is collected, how it is used, and the measures in place to protect their privacy. This transparency helps build trust and ensures that young users are aware of how their information is handled ("Fundamentals for a Child-Oriented Approach to Data Processing" [i.12]).

- Enhanced security: Implementing enhanced security measures specifically tailored to protect the data of underage users is crucial. This includes secure data storage, encrypted communication channels, and regular security audits ("Privacy; a foundational concept for age verification" [i.29]).

- Data deletion: Ensure that personal data is deleted immediately after verification to prevent unauthorized access and use of the data ("Privacy; a foundational concept for age verification" [i.29]).

- Pseudonymization: Use pseudonymization techniques, such as data masking and hashing, to protect personal data, ensuring that it cannot be directly attributed to an individual without additional information ("PAS 1296:2018 Online age checking. Provision and use of online age check services. Code of Practice" [i.16]).

b) Access control and content limitation:

- Prevent access to harmful content: Mechanisms should be in place to prevent underage users from accessing content that is harmful or inappropriate. This includes using effective age verification systems and content filters ("Draft Spanish law on the protection of children and adolescents in the digital environment" [i.14]).

- Parental control features: Providing robust parental control features allows parents to limit access to certain content or set time limits for use, thereby helping to create a safer online environment for their children ("Draft Spanish law on the protection of children and adolescents in the digital environment" [i.14]).

c) Transparency and information provision:

- Risk information: Clear, age-appropriate information about the risks associated with internet use should be provided to underage users. This helps them understand potential dangers and how to navigate the digital world safely ("Fundamentals for a Child-Oriented Approach to Data Processing" [i.12]).

- Digital literacy support: Supporting the development of digital literacy skills in children is essential. Educational programs and resources should be made available to help them understand how to use technology responsibly and safely ("Draft Spanish law on the protection of children and adolescents in the digital environment" [i.14]).

d) Rights and safeguards:

- Respect Children's Rights: Ensuring that children's rights are respected and protected in digital environments is a fundamental requirement. This includes their right to privacy, freedom of expression, and protection from exploitation ("Draft Spanish law on the protection of children and adolescents in the digital environment" [i.14]).

- Redress Mechanisms: Providing clear channels for children to seek redress or challenge decisions related to age verification is important for maintaining trust and ensuring fair treatment ("Age Assurance: Guiding Principles and Best Practices" [i.32]).

e) Inclusion and accessibility:

- Accessible Systems: Age assurance systems should be designed to be inclusive and accessible to all underage users, regardless of their socioeconomic status, race, or other characteristics. This ensures that no child is left unprotected due to systemic barriers ("Age Assurance: Guiding Principles and Best Practices" [i.32]).

- Avoid Discrimination: Age assurance systems are meant to prevent discrimination against marginalized groups of children, ensuring equal protection and access to digital services for all ("UNICEF Digital Age Assurance Technologies and Children's Rights" [i.27]).

f) Implementation and compliance:

- Compliance with Legal Standards: It is critical to ensure that age verification systems comply with GDPR [i.4] and other relevant regulations. This compliance helps protect user data and maintain the integrity of the verification process ("Recommendation 7: Check the age of the child and parental consent while respecting the child's privacy" [i.10]).

- International Standards: Adhering to international standards, such as IEEE 2089.2021 [i.17] ensures that age verification systems meet globally recognized benchmarks for quality and security ("PAS 1296:2018 Online age checking. Provision and use of online age check services. Code of Practice" [i.16]).

- Privacy by Design: Implementing privacy-by-design principles into age verification systems ensures that privacy considerations are integrated into the development and operation of these systems from the outset ("Age Assurance and Age Verification Tools: Takeaways from CIPL Roundtable" [i.31]).

7.2 Parents of underage users' requirements

This clause details the requirements for parents of underage users of internet services, highlighting how age verification systems and privacy measures can support them. The following requirements have been identified:

a) Parental consent mechanisms:

- Robust consent verification: Develop and implement secure systems to obtain and verify parental consent for underage users. This includes using multi-factor authentication or secure verification methods like government-issued ID checks ("Fundamentals for a Child-Oriented Approach to Data Processing" [i.12]; "Age Assurance: Guiding Principles and Best Practices" [i.32]).

- Specific consent: Ensure that parental consent is specific to particular data processing activities, allowing parents to make informed decisions about their children's data ("Methods for Obtaining Parental Consent and Maintaining Children Rights" [i.33]).

b) Transparency and information provision:

- Clear information: Provide clear, age-appropriate privacy information to parents about how age verification works, what data is collected, how it is used, and the measures in place to protect their children's privacy ("Privacy; a foundational concept for age verification" [i.29]).

- Regular reporting: Maintain transparency by periodically reporting on age assurance practices to parents and other stakeholders ("Age Assurance: Guiding Principles and Best Practices" [i.32]).

c) Privacy and Data Protection:

- Privacy-preserving methods: Encourage the use of privacy-preserving age verification methods that do not require personal identification documents from parents. These methods should minimize data collection and adhere to privacy by design principles ("Online age verification: balancing privacy and the protection of minors" [i.11]).

- Data minimization: Design parental consent mechanisms with privacy in mind, ensuring that only [i.12] necessary data is collected and processed ("UNICEF Digital Age Assurance Technologies and Children's Rights" [i.27]).

ci) Support and education:

- Educational resources: Provide parents with resources about the importance of age verification and how to manage their children's online presence effectively ("Age Assurance and Age Verification Tools: Takeaways from CIPL Roundtable" [i.31]).

- User-friendly tools: Develop user-friendly age assurance tools that are accessible and easily understandable for parents ("A Multi-Stakeholder Dialogue on Age Assurance" [i.31]).

cii) Rights and safeguards:

- Redress mechanisms: Create mechanisms for parents to easily revoke or manage their consent at any time, with changes taking effect promptly across all relevant online services.

- Parental control tools: Incorporate systems that include user-controlled mechanisms such as parental control tools to manage and restrict access to inappropriate content for minors ("Online age verification: balancing privacy and the protection of minors" [i.11]).

ciii) Compliance and governance:

- Legal Compliance: Ensure that age verification systems comply with GDPR [i.4] and other relevant legal frameworks, providing parents with confidence in the online services their children use ("Recommendation 7: Check the age of the child and parental consent while respecting the child's privacy" [i.10]).

- International standards: Adhere to international standards such as IEEE 2089.2021 [i.17] to ensure rigorous testing and certification of age verification systems ("Privacy; a foundational concept for age verification" [i.29]).

7.3 Adult users of internet services and recipients of information groups requirements

This clause details the requirements for adult users of internet services, emphasizing the importance of robust privacy measures, clear information provision, and secure data handling. The following requirements have been identified:

a) Privacy and data protection:

- Explicit consent: Obtain explicit consent from users before collecting any personal data. Ensure data minimization by collecting only the necessary information for age verification and other purposes.

- Privacy-preserving methods: Utilize advanced cryptographic methods, such as group signatures and zero-knowledge proofs, to allow users to prove their age without revealing any other personal information ("Demonstration of a privacy-preserving age verification process" [i.20]).

- Data security: Implement robust security measures to protect user data from unauthorized access and breaches. Ensure that all data collected is stored securely and used solely for the intended purposes ("Privacy; a foundational concept for age verification" [i.29]).

b) Transparency and information provision:

- Clear information: Provide transparent information to users about how age assurance tools are used, what data is collected, and the measures in place to protect their privacy. This includes details on data sources and how age verification is conducted ("UNICEF Digital Age Assurance Technologies and Children's Rights" [i.27]).
- User control: Ensure that users have control over their data exchanges and the ability to manage their age verification tokens securely on their devices. Provide mechanisms for users to revoke consent and delete their data as needed.

c) Inclusion and accessibility:

- Accessible systems: Design age assurance systems to be inclusive and accessible to all adult users, including those without access to government IDs or advanced technology. Ensure that these systems do not discriminate against marginalized groups ("Measurement of Age Assurance Technologies" [i.23]).
- Non-intrusive verification: Develop solutions that effectively verify age without being overly invasive, ensuring that privacy and convenience are balanced ("Keeping Kids Safe Online: How Should Policymakers Approach Age Verification" [i.26]).

d) Rights and safeguards:

- Redress mechanisms: Provide clear channels for users to seek redress or challenge decisions related to age verification. Ensure that these mechanisms are easily accessible and user-friendly ("A Multi-Stakeholder Dialogue on Age Assurance" [i.31]).
- Compliance with legal standards: Ensure compliance with GDPR [i.4] and other relevant legal frameworks to protect user data and maintain the integrity of age verification processes ("Recommendation 7: Check the age of the child and parental consent while respecting the child's privacy" [i.10]).

e) Implementation and governance:

- International standards: Adhere to international standards such as IEEE 2089.2021 [i.17] to ensure rigorous testing and certification of age verification systems. Ensure continuous improvement and auditing of these systems to maintain their effectiveness and security ("PAS 1296:2018 Online age checking. Provision and use of online age check services. Code of Practice" [i.16]).
- Privacy by design: Integrate privacy-by-design principles into all age assurance solutions, ensuring that privacy considerations are a core part of the system development and implementation process ("Age Assurance and Age Verification Tools: Takeaways from CIPL Roundtable" [i.30]).

7.4 Providers of age verification services and national authorities providing age verification solutions

As digital services continue to expand, the need for reliable age verification systems becomes increasingly important. Providers of age verification services and national authorities need to ensure that these systems are not only effective but also respect user privacy and comply with legal requirements. This clause details the essential requirements for these stakeholders:

a) Privacy and data protection:

- Data minimization: Collect only the necessary data required for verifying age and ensure that this data is stored securely and used solely for the purpose of age verification ("Privacy; a foundational concept for age verification" [i.29]).
- Privacy-preserving methods: Utilize advanced cryptographic methods, such as group signatures and zero-knowledge proofs, to verify age without revealing other personal information ("Demonstration of a privacy-preserving age verification process" (CNIL) [i.20]).

- Data security: Implement robust security measures to protect personal data from unauthorized access and breaches. This includes encryption and regular security audits ("Technical Requirements for Data Protection and Privacy" (The Age Check Certification Scheme) [i.36]).

b) Transparency and information provision:

- Clear information: Provide transparent and accessible information to users about how age verification works, what data is collected, and the measures in place to protect their privacy ("Guidance on age assurance and other Part 5 duties for service providers publishing pornographic content on online services" (Ofcom) [i.9]).

- User control: Ensure that users can manage their data, including the ability to revoke consent and delete their information as needed ("Age assurance for the Children's code" (Information Commissioner Office, ICO) [i.15]).

c) Compliance and governance:

- Legal Compliance: Ensure that age verification systems comply with GDPR [i.4] and other relevant regulations, such as the European Digital Identity Wallet (EUDI Wallet) Regulation ("Decalogue of principles: Age verification and protection of minors" (AEPD, Spain) [i.13]).

- International Standards: Adhere to international standards such as IEEE 2089.2021 [i.17] ensuring rigorous testing and certification of age verification system ("IEEE Standard for Online Age Verification" (IEEE) [i.18]).

d) Implementation and best practices:

- Risk-based approach: Develop risk-based assurance approaches tailored to different levels of online risk exposure ("Keeping Kids Safe Online: How Should Policymakers Approach Age Verification?" (The Centre for Growth and Opportunity, Utah State University) [i.26]).

- Regular audits: Conduct regular audits and reviews of age verification systems to ensure ongoing compliance and effectiveness ("Measurement of Age Assurance Technologies" (ICO and Ofcom) [i.23]).

e) Ethical guidelines and user rights:

- Ethical standards: Implement stringent ethical guidelines to protect user privacy and rights during the age verification process ("Global Age Assurance Standards Summit 2024- Compendium" (The Age Check Certification Scheme) [i.36]).

- User-friendly solutions: Design age verification solutions that are accessible and user-friendly, considering diverse user demographics, including children, adults, and individuals with disabilities ("IEEE Standard for an Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children" (IEEE) [i.17]).

7.5 Service/products providers subject to age verification obligations

This clause details the essential requirements for service providers who need to obtain age information, emphasizing the importance of privacy, data protection, and compliance with legal standards.

a) Privacy and data protection:

- Data minimization: Ensure that the age verification process collects only the minimum necessary data from users, strictly limiting this to what is essential for verifying age.

- Preserving methods: Implement a privacy-preserving system where a third-party verifier conducts the age verification process without revealing the user's identity or the identity of the website requesting the information ("Demonstration of a privacy-preserving age verification process" (CNIL) [i.20]).

- Data security: Implement robust security measures to protect personal data from unauthorized access and breaches. This includes encryption and regular security audits ("The Age Check Certification Scheme" [i.36]).

b) Transparency and information provision:

- Clear information: Provide transparent and accessible information to users about how age verification works, what data is collected, and the measures in place to protect their privacy ("Guidance on age assurance and other Part 5 duties for service providers publishing pornographic content on online services" (Ofcom) [i.9]).
- Parental consent: Obtain parental consent for minors to access certain content or services, ensuring that this consent is specific and informed (" Spanish draft LO" [i.14]).

c) Compliance and governance:

- Legal compliance: Ensure that age verification systems comply with GDPR [i.4] and other relevant regulations, such as the European Digital Identity Wallet (EUDI Wallet) Regulation ("Decalogue of principles: Age verification and protection of minors" (AEPD, Spain) [i.13].
- International standards: Adhere to international standards such as IEEE 2089.2021 [i.17] ensuring rigorous testing and certification of age verification systems ("IEEE Standard for Online Age Verification" [i.18]).

d) EUDI wallet and audits:

- EUDI wallet: Comply with technical specifications for age verification mechanisms, including those outlined in the EUDI Wallet Regulation (EU) 2024/1183 [i.2] ("Spanish draft LO" [i.14]).
- Regular audits: Conduct regular audits and reviews of age verification systems to ensure ongoing compliance and effectiveness ("Measurement of Age Assurance Technologies" (ICO and Ofcom) [i.23]).

e) Ethical guidelines and user rights:

- Ethical standards: Implement stringent ethical guidelines to protect user privacy and rights during the age verification process ("Global Age Assurance Standards Summit 2024 - Compendium" (The Age Check Certification Scheme) [i.36].
- User-friendly solutions: Design age verification solutions that are accessible and user-friendly, considering diverse user demographics, including children, adults, and individuals with disabilities. ("IEEE Standard for an Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children" [i.17]).

8 Conclusions

The present document provides a comprehensive overview of stakeholder requirements for age verification, essential for developing a standardized approach to age verification and age estimation solutions. This will help align efforts across various sectors and jurisdictions, ensuring the protection of minors online while maintaining compliance with legal and regulatory requirements.

Underage users of internet services require systems that reliably verify age using secure methods that protect personal data. Implementation of privacy-preserving verification methods ensures anonymity, and only the essential data necessary for age verification should be collected. The age verification processes should be seamless and not create barriers for users. Parents of underage users need systems that facilitate obtaining and verifying parental consent, ensuring both parents' involvement where applicable. Transparency is crucial, providing clear, age-appropriate information about the data being collected and how it will be used. Tools should be available to allow parents to manage their children's online activities and revoke consent if necessary. Additionally, resources should inform parents about safe online practices and the importance of privacy.

Adult users require assurances that any data collected during age verification will be protected and not misused. Clear information about the age verification process and data handling practices is essential. Providers of age verification services and national authorities are obliged by GDPR [i.4], the Digital Services Act [i.1], and other relevant legal frameworks. Developing systems that can work across various platforms and jurisdictions, implementing robust security measures to protect data during transmission and storage, and ensuring continuous oversight and updates to age verification methods to address emerging challenges are crucial.

Service providers subject to age verification obligations have the obligation to ensure that the content provided is suitable for the verified age group and comply with national and international regulations regarding age-restricted content and services. Age verification should not hinder the user experience and should be integrated smoothly into the service. Additionally, integrating robust parental control settings to manage access to content is necessary.

The plan for standardization of age verification solutions involves establishing unified standards with comprehensive guidelines that detail the technical and procedural requirements for age verification systems, ensuring consistency across platforms and regions. Encouraging the development of interoperable systems that can be easily adopted by service providers and verified by national authorities is important. Ensuring all age verification solutions comply with GDPR [i.4], eIDAS2 [i.2], and other relevant laws provides a legal framework for data protection and user privacy. Regular audits and compliance checks by authorities help maintain the integrity of age verification processes. Fostering collaboration among stakeholders, including service providers, regulatory bodies, parents, and user advocacy groups, ensures the solutions meet diverse needs and concerns. Conducting educational campaigns informs stakeholders about the importance of age verification and how to use the tools effectively. Establishing feedback mechanisms to continuously gather input from stakeholders and refine age verification methods, staying updated with technological advancements, and incorporating innovative solutions to address new challenges in age verification and estimation are also necessary.

History

Document history		
V1.1.1	September 2024	Publication
V1.1.2	December 2024	Publication