AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

COURTESY TRANSLATION

RESOLUTION NO. 96/25/CONS

ADOPTION OF TECHNICAL AND PROCEDURAL METHODS FOR VERIFYING THE AGE OF USERS IN IMPLEMENTATION OF LAW NO. 159 OF NOVEMBER 13, 2023

THE AUTHORITY

AT its Council meeting on April 8, 2025;

HAVING REGARD to Law No. 481 of November 14, 1995, containing *"Rules for competition and regulation of public utility services. Establishment of the Regulatory Authority for Public Utility Services*";

HAVING REGARD to Law No. 249 of July 31, 1997, *establishing the Authority for Guarantees in Communications and rules on telecommunications and* radio *and* television *systems*, hereinafter referred to as *the Authority*;

HAVING REGARD TO the Personal Data Protection Code, containing provisions for the adaptation of national legislation to Regulation (EU) 2016/679 (Legislative Decree No. 196 of June 30, 2003, as amended by Legislative Decree No. 101 of August 10, 2018, hereinafter referred to as the "Code");

HAVING REGARD TO Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 (GDPR - *General Data Protection Regulation* - or Regulation);

HAVING REGARD TO Legislative Decree No. 259 of August 1, 2003, containing *the "Electronic Communications* Code" (hereinafter also referred to as the "Code"), as last amended by Law No. 193 of December 16, 2024, containing *the "Annual Law for the Market and Competition 2023*";

HAVING REGARD TO Legislative Decree No. 207 of November 8, 2021, on *the "Implementation of Directive (EU) 2018/1972 of the European Parliament and of the Council of December 11, 2018, establishing the European Electronic Communications Code (recast)*;

HAVING REGARD TO Legislative Decree No. 208 of November 8, 2021, on *'Implementation of Directive (EU) 2018/1808 of the European Parliament and of the Council of November 14, 2018, amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation, or administrative action in Member States concerning the provision of audiovisual media services in view of market* developments', as amended by Legislative Decree No. 50 of March 25, 2024, containing *"Supplementary and corrective provisions to Legislative Decree No. 208 of November 8, 2021, containing the consolidated text on audiovisual media services in*

view of market developments, implementing Directive (EU) 2018/1808 amending Directive 2010/13/EU";

HAVING REGARD TO Decree Law No. 123 of September 15, 2023, containing "*Urgent measures to combat youth hardship, educational poverty, and juvenile crime, as well as for the safety of minors in the digital environment*," as converted, with amendments, by Law No. 159 of November 13, 2023, and, in particular, Articles *13-bis and* 15 (hereinafter also referred to as the Decree);

HAVING REGARD TO Regulation (EU) No. 2022/2065 of the European Parliament and of the Council of October 19, 2022, on a single market for digital services and amending Directive 2000/31/EC (Digital Services Regulation, hereinafter also referred to as DSA);

HAVING REGARD TO Regulation 2024/1183 of the European Parliament and of the Council of April 11, 2024, amending Regulation (EU) No. 910/2014 as regards the establishment of the European Digital Identity Framework;

HAVING REGARD TO Resolution No. 298/23/CONS of November 22, 2023, containing *"Regulations implementing Article 41, paragraph 9, of Legislative Decree No. 208 of November 8, 2021, concerning programs, user-generated videos or audiovisual commercial communications aimed at the Italian public and conveyed by a video-sharing platform whose provider is established in another Member State" and* the related notification to the European Commission as a technical regulation;

HAVING REGARD TO Resolution No. 9/23/CONS of January 25, 2023, concerning *the "Adoption of guidelines for the implementation of Article 7-bis of Decree-Law No. 30 of April 30, 2020,*
No. 28 on "systems for protecting minors from the risks of cyberspace";

HAVING REGARD TO Resolution No. 223/12/CONS of April 27, 2012, concerning *the "Adoption of the new Regulation on the organization and functioning of the Communications Regulatory Authority"* (hereinafter, "Regulations")", as last amended by Resolution No. 58/25/CONS of March 6, 2025;

HAVING REGARD TO Resolution No. 401/10/CONS of July 22, 2010, on *"Regulation of the timing of proceedings*," as amended and supplemented;

HAVING REGARD TO Resolution No. 107/19/CONS of April 5, 2019, on the *"Adoption of regulations concerning consultation procedures in proceedings falling within the competence of* the Authority";

HAVING REGARD TO the memorandum of understanding signed on April 12, 2023, between the Authority and the Data Protection Authority, whereby they undertake to launch a series of initiatives useful for the performance of their respective tasks, through the exchange of data and information, the creation of study groups, and the launch of joint public consultations, with particular regard to the protection of minors *online* and political advertising;

HAVING REGARD, in particular, to the joint working group set up by the two Authorities to promote a code of conduct that will lead digital platforms to adopt systems for verifying the age of young users accessing *online* services;

HAVING REGARD TO Resolution No. 9/24/CONS of January 10, 2024, which ordered *the "Initiation of preliminary proceedings aimed at implementing Article 13-bis of Decree-Law No. 123 of September 15, 2023, No. 123 containing urgent measures to combat youth hardship, educational poverty, and juvenile crime, as well as for the safety of minors in the digital environment," converted, with amendments, by Law No. 159 of November 13, 2023*";

HAVING REGARD to Article 1 of the aforementioned resolution and, in particular, paragraph 1, which initiated the preliminary investigation procedure aimed at implementing the provisions of paragraph 3 of Article 13-bis of Decree-Law No. 123/2023, converted, with amendments, by Law No. 159/2023, through the approval of a measure regulating the technical and procedural methods that the subjects identified by the law are required to adopt to verify the age of majority of users;

CONSIDERING that paragraph 4 of the same article provides for a 30-day public consultation on the Authority's resolution, subject to obtaining the opinion of the Data Protection Authority;

HAVING REGARD TO Resolution No. 61/24/CONS of March 6, 2024, concerning *"Launch of the public consultation referred to in Article 1, paragraph 4, of Resolution No. 9/24/CONS aimed at adopting a measure on the technical and procedural methods for verifying the age of users in implementation of Law No.* 159 *of November 13, 2023*";

CONSIDERING that the current legislation – also specifically referring to the role of the Authority – repeatedly refers to the need to implement *age verification* mechanisms, establishing that minors are entitled to a higher level of protection from content that could harm their physical, mental, or moral development, including by introducing stricter measures for all information society services;

CONSIDERING that the European Commission supports and promotes the implementation of rules aimed at protecting minors *online* and that Article 28 of the DSA requires all providers of *online* platforms accessible to minors to take appropriate and proportionate measures to ensure a high level of privacy, security, and protection of minors, primarily through the activation of age verification mechanisms;

CONSIDERING also that, pursuant to Article 35(1)(j) letter j) of the DSA, providers of very large *online* platforms and very large *online* search engines shall take measures to mitigate systemic risks, including "*targeted measures to protect the rights of minors, including age verification and parental control tools, or tools to help minors report abuse or obtain support, as appropriate*";

HAVING REGARD to Article 8 of the GDPR, which sets out the conditions applicable to the consent of minors in relation to information society services;

HAVING REGARD TO the powers specifically assigned to the Authority by TUSMA and, in particular:

- from paragraph 7 of Article 41, which provides that: ***Without prejudice to the provisions of paragraphs 1, 2, 3, 4, 5, and 6, the free movement of programs, user-generated videos, and audiovisual commercial communications conveyed by a video-sharing platform whose provider is established in another Member State and directed at the Italian public may be restricted, by order of the Authority,*** *in accordance with the procedure set out in Article 5, paragraphs 2, 3, and 4 of Legislative Decree No. 70 of 2003, for the following purposes: a) the protection of minors from content that may harm their physical, mental, or moral development in accordance with Article 38, paragraph 1;*

- paragraphs 1 and 6 of Article 42, where they provide that: *1. Providers of video-sharing platforms subject to Italian jurisdiction* ***must take appropriate measures to protect:***

a) minors from programs, user-generated videos, and audiovisual commercial communications that may harm their physical, mental, or moral development, in accordance with Articles 37 and 43;

[omissis]

6. For the purposes of protecting minors referred to in paragraph 1, letter a), the most harmful content is subject to the most stringent access control measures.

CONSIDERING in particular that, pursuant to paragraph 7 of Article 42 of the TUSMA:

7. ***Video-sharing platform providers are in any case required*** *to:*

[omissis]

f) ***set up systems to verify, in compliance with the legislation on personal data protection, the age of users of video sharing platforms*** *with regard to content that may be harmful to the physical, mental, or moral development of minors;*

[omissis]

h) equip themselves with parental control systems under the supervision of the end user with regard to content that may be harmful to the physical, mental, or moral development of minors;

CONSIDERING it appropriate, therefore, to assess, within the scope of the public consultation launched by Resolution No. 61/24/CONS, whether the age verification system outlined in the document submitted for consultation, through the indication of general requirements and *performance* indicators, is effective, suitable, and functional for application, in accordance with the regulatory context referred to above, also with reference to additional types of content that could be harmful to the physical, mental, or moral development of minors;

HAVING REGARD to the results of the public consultation set out in **Annex C** and the regulatory and legislative review set out in **Annex B** to this measure, which form an integral and substantial part thereof;

CONSIDERING it appropriate to clarify, in view of the comments made by some of those who took part in the public consultation, that the rules on the technical and procedural methods for verifying the age of users, which are approved by this resolution in implementation of Article 13-bis of Decree-Law No. 123/2023, converted, with amendments, by Law No. 159/2023, **must be adopted by website operators and video-sharing platform providers that disseminate pornographic images and videos in Italy, wherever they are established;**

CONSIDERING, for all intents and purposes, that in light of the aforementioned regulatory framework and the results of the consultation itself, the technical and procedural methods for verifying the age of majority of users approved by this resolution in implementation of the aforementioned decree-law (as converted into law) **are highly recommended, as they are effective, appropriate, proportionate, and functional, for their use by parties other than those directly regulated herein and with reference to additional types of content, beyond those of a pornographic nature, which could nonetheless be harmful to the physical, mental, or moral development of minors, such as the categories provided for in Resolution 9/03/CONS;**

HAVING REGARD TO provision no. 88 of February 8, 2024, whereby, pursuant to Article 58, paragraph 3, letter b) of Regulation (EU) 2016/679, the Italian Data Protection Authority (Garante), having examined the draft measure submitted by the Authority, expressed a favorable opinion on the launch of the public consultation envisaged by the Authority in its Resolution No. 9/24/CONS of January 10, 2024;

HAVING REGARD TO measure no. 470 of July 17, 2024, whereby, pursuant to Article 58, paragraph 3, letter b) of Regulation (EU) 2016/679, the Guarantor expressed a favorable opinion on the text of the draft measure, transmitted by Agcom with a note dated June 12, 2024, following the conclusion of the aforementioned public consultation, on condition that the additions indicated in the separate note sent together with the aforementioned measure are incorporated;

CONSIDERING that, at its meeting on September 24, 2024, the Authority approved the final draft measure governing the technical and procedural methods for verifying the age of users of online pornographic content;

HAVING REGARD TO the favorable opinion of the Data Protection Authority sent by note dated July 25, 2024;

CONSIDERING that the final draft measure was notified on October 16, 2024, to the European Commission as a technical rule pursuant to Directive (EU) 2015/1535 (Notification 2024/578/IT). The notification suspended the deadline for the adoption of the final measure for a period of three months until January 17, 2025;

CONSIDERING that, in relation to the notified draft, on October 28, 2024, the Commission requested additional information from the Italian authorities in order to obtain clarification on the measures contained in the notified draft, to which the Authority responded by providing its clarifications in a note sent on November 12, 2024;

CONSIDERING that on January 16, 2025, the European Commission sent a detailed opinion pursuant to Article 6(2) of the aforementioned Directive (EU) 2015/1535;

CONSIDERING that the adoption of a detailed opinion means that the Member State that drafted the technical regulation in question is required to postpone its adoption for four months from the date of notification. Therefore, the new deadline for issuing the measure is February 17, 2025;

CONSIDERING that the Commission has drawn the attention of the Italian authorities to the fact that, under the same provision, the Member State receiving a detailed opinion is required to inform the Commission of the measures it intends to take in response to that opinion;

HAVING REGARD TO the outcome of the board meeting of February 5, 2025, during which the Authority approved the additions and amendments made to the notified draft in order to take full account of the comments made by the Commission in the aforementioned detailed opinion, to which it intended to respond in a timely manner;

HAVING REGARD TO the Authority's response to the Commission sent on February 24, 2025, with the draft measure containing the technical rules amended in accordance with the recommendations of the aforementioned opinion attached;

CONSIDERING the following:

1. Following the detailed opinion issued by the European Commission

Firstly, it is important to note that the Commission agreed with the objective pursued by AGCOM through the notified project, which is to protect minors online, in particular from pornographic content that could harm their health and physical, mental, and moral development. These objectives are in line with those of the European legal framework for online services, in particular Regulation (EU) 2022/2065 (hereinafter the 'Digital Services Act' or DSA) and Directive 2000/31/EC (e-Commerce Directive).

As emphasized by the Commission, the aforementioned regulation is directly applicable without implementing measures in all Member States and provides an effective regulatory framework at Union level with regard to some of the objectives pursued by the notified project.

Therefore, taking note of the need to ensure the harmonized implementation of the aforementioned regulation and the necessary compliance of the project with the aforementioned directive, the Authority has decided, on a preliminary basis, to proceed with an overall simplification of the regulatory framework of the proposed project in order to avoid the risk of encountering the critical issues raised by the Commission.

In this regard, definitions that merely repeat the provisions of directly applicable European legislation, which falls within the competence of the Commission itself, have also been eliminated.

1.1 Description of the measures introduced to take account of the detailed opinion :

a) Application of Article 3(1), (2), and (4) of Directive 200/31/EC and introduction of a list of entities

Given that the provisions of the notified draft apply to information society service providers offering their services on Italian territory, regardless of the Member State in which they are established, it seems appropriate to clarify at the outset that this scope of application (both subjective and objective) is defined by the primary legislation that this Authority is responsible for implementing[1].

Therefore, it is up to the Authority to determine the *technical and procedural methods that the subjects referred to in paragraph 2 are required to adopt to verify the age of users*, an aspect on which the opinion did not raise any objections.

That said, it is noted that the Commission also pointed out that the Member State may, if necessary, derogate from the principle of control by the Member State of origin for the reasons strictly listed in Article 3(4)(a) of Directive 2000/31/EC and in compliance with the substantive and procedural requirements set out in Article 3(4)(a) and (b) thereof.

Indeed, a similar clarification has already been made in relation to the adoption of a different regulation (the one on *video sharing platforms* implementing Article 41 of TUSMA referred to in AGCOM Resolution No. 289/24/CONS) on which the Commission, also in light of the clarifications

[1] Article *13-bis* of Decree-Law No. 123 of September 15, 2023, provides (Caivano Decree), in paragraphs 2 and 3, that:

2. Without prejudice to the provisions of Article 42 of Legislative Decree No. 208 of November 8, 2021, website operators and video sharing platform providers that distribute pornographic images and videos in Italy are required to verify that users are of legal age in order to prevent minors under the age of 18 from accessing pornographic content.

3. The Communications Regulatory Authority shall establish, within sixty days of the date of entry into force of the law converting this decree, by its own measure, after consulting the Data Protection Authority, the technical and procedural methods that the subjects referred to in paragraph 2 are required to adopt to verify the age of users, ensuring a level of security appropriate to the risk and compliance with the minimization of personal data collected for the purpose.

provided by the Authority, did not raise any doubts as to compliance with the European regulatory framework, despite the fact that the rules apply regardless of the establishment of the VSP.

Consequently, in order to overcome the critical issues identified, the Authority intends **to limit the scope of application of the provisions introduced by the notified draft to information society services established in Italy or outside the European Union (**see Article 1, paragraph 1, of the draft) and **to provide for extension to entities established in other Member States in accordance with the criteria and procedures set out in Article 3 of Directive 2000/31/EC (**see Article 1, paragraph 3, of the draft).

Therefore, when the conditions set out in paragraph 4(a) of Article 3 of Directive 2000/31/EC are met, the measures referred to in paragraph 5 of Article *13-bis* of the Caivano Decree shall apply following the procedures laid down in paragraph 4(a)
b) or, where applicable, paragraph 5 of the same Article 3. In particular, the measure may be adopted by the Authority only after it has addressed the Member State in which the service provider is established, requesting it to adopt the measure, and the latter has not taken action or the action taken has not been considered adequate and, in any case, after notifying the Commission and the Member State of its intention to adopt the aforementioned measure.

Furthermore, in order to avoid regulatory provisions establishing general and abstract obligations imposed on broad and undefined categories of service providers, regardless of their place of establishment, it has been clarified, from a subjective point of view, that the **subjects to whom the notified draft applies are website operators and video-sharing platforms that disseminate pornographic images and videos in Italy.**

It should also be noted that, on the basis of the criteria set out in Article 1, paragraph 2, of Annex A, the Authority intends to draw up a **list** (compiled and updated periodically, and communicated to the European Commission) identifying the entities to which the notified draft applies (see Article 1, paragraph 1, last sentence of the Guidelines).

It has been provided (in Article 4 of the Guidelines) that **the provisions introduced will also apply to website operators and video-sharing platforms that disseminate pornographic images and videos in Italy, regardless of the Member State of establishment, three months after the publication of the** above-mentioned **list**.

b) Full harmonization of the Digital Services Regulation through the introduction of a review clause and the elimination of additional transparency obligations.

As regards the possible critical issues related to the need to ensure full harmonization of the notified measure with the DSA, avoiding any risk of overlap, particularly with regard to minors, it is known that the Commission will adopt

guidelines on the application of Article 28 of the Regulation on the adoption of *appropriate and proportionate measures to ensure a high level of privacy, security, and protection of minors on their service.*

On the basis of this awareness, the Authority has introduced certain amendments to ensure full consistency with the DSA.

It should nevertheless be noted that the notified measure, **which falls within the scope of Article *28b*(6) of the AVMS Directive, does not appear to overlap with the Digital Services Regulation or to merely provide the minimum requirements that the system must provide for in order to protect privacy.**

These requirements are not regulated by the DSA, as recognized by the Commission when it observes that *'**in the absence of an EU-wide solution for verifying the age of users, any transitional national solution should remain in line with EU law, including Article 3 of Directive 2000/31/EC, and also provide for a mechanism to revoke or repeal national measures that become redundant once the European technical solution is implemented.***

The Commission therefore does not rule out national transitional solutions, **provided that they comply with Union law, including Article 3 of Directive 2000/31/EC.**

Therefore**, an explicit mechanism has been introduced in the final provisions to ensure compliance with subsequent European legislation: where necessary, the Authority will amend, revoke, or repeal measures adopted at national level with regard to entities established in other Member States, with effect from the date of entry into force of the guidelines adopted pursuant to Article 28 of the DSA.**

In this regard, it should be reiterated that the Authority attaches considerable importance to the need for coordination and enhancement of the exchange of experiences between different countries, actively participating in specific European working groups on the protection of minors and, more generally, on the practical application of the DSA.

The need for harmonization is also ensured by the entry into force regime of the notified draft which, pursuant to Article *13-bis*, paragraph 4, of the Caivano Decree, provides that the provisions in question shall enter into force six months after the adoption of the measure by the Authority.

Further harmonization requirements have led this Authority, in view of the comments made in its opinion, to eliminate the transparency obligations that the Commission considered to be additional to the directly applicable European legislation[2].

[2] This refers to the obligations set out in the previous version of Article 2 of the notified draft, i) to report to the Communications Regulatory Authority and ii) to increase transparency towards users with regard to information on online content moderation through the age assurance mechanism.

The following provisions were therefore removed from the final measure:

Obligations to report to the Authority

Website operators and video-sharing platform providers that disseminate pornographic images and videos in Italy must notify the Authority of the third parties entrusted with age verification (independent third parties), together with a report containing all relevant information on the party, the age verification method, and the reasons for the choice, for the purposes of the Authority's supervisory activities.

i Transparency:

ii *Regulated entities should be transparent with users regarding the systems and data processed and the purposes for which they are used, providing simple, clear, and comprehensive explanations for both adults and minors.*

iii *Regulated entities must make available on their websites data relating to the accuracy and effectiveness of the age assurance systems used, reporting the metrics and parameters used in the assessment as well as the results obtained.*

c) Modification of the monitoring and forecasting system for cooperation.

The Commission noted that "*the notified draft entrusts the supervision and enforcement of its provisions, including those falling within the fully harmonized area of the Digital Services Regulation, to the Communications Regulatory Authority. This supervision and enforcement system under the notified draft would also apply to service providers outside Italian jurisdiction and to VLOPs to the extent that they fall within the scope of the notified draft*."

In light of these observations, the Authority has consequently amended the notified draft, taking into account the provisions of the DSA (Articles 56 and 57).

2 Conclusions

That said, the amendments and additions made to the draft are summarized below:

1. Simplification of the regulatory framework of the measure in accordance with the necessary full harmonization with the relevant European legislation;

2. Clarification of the subjective and objective scope of application of the measure, specifying the operators of websites and video-sharing platforms that disseminate pornographic images and videos in Italy;

3. Introduction of the express reference (for non-Italian entities established within the EU) to the conditions and procedures referred to in Article 3 of Directive 2000/31/EC ("Directive on electronic commerce"). It follows that the measures referred to in paragraph 5 of Article *13-bis* of the Caivano Decree apply following the procedure laid down in the aforementioned provision of the Directive.

4. Provision for the preparation, in a manner deemed transparent and objective, of a list by the Authority for the purpose of identifying the persons subject to the obligation and provision for a three-month period for the applicability of the measure to persons established in another Member State;

5. Elimination of additional transparency obligations with respect to directly applicable European legislation;

6. Without prejudice to the procedure provided for in the e-commerce directive, harmonization of monitoring and supervisory activities and introduction of cooperation at European level;

7. Provision, in the final provisions, for an express mechanism to amend, revoke, or repeal, where necessary, measures adopted at national level with regard to entities established in other Member States, with effect from the date of entry into force of the guidelines adopted pursuant to Article 28 of Regulation (EU) 2022/2065, in order to comply with the European legislation that has come into force;

8. Provision for a special regime for the entry into force of the measure, also with a view to ensuring full European harmonization.

HAVING HEARD the report of Commissioner Laura Aria, rapporteur pursuant to Article 31 of the Regulation on the organization and functioning of the Authority;

RESOLVES

Sole Article

1. As part of the preliminary investigation aimed at implementing the provisions of paragraph 3 of Article 13-bis of Decree-Law No. 123/2023, converted, with amendments, by Law No. 159/2023, referred to in Article 1 of Resolution No. 9/24/CONS, the technical and procedural methods that website operators and video-sharing platforms that disseminate pornographic images and videos in Italy, whether established in Italy or in another Member State, are required to adopt in order to verify the age of users are established, **as set out in Annex A**, which forms an integral and substantial part of this resolution.

2. The results of the public consultation and the regulatory review are set out in **Annexes C and B** to this resolution, which form an integral and substantial part thereof.
3. The Authority shall set up a technical committee to monitor and analyze technical, legislative, and regulatory developments in the field of *age assurance* systems.
4. The Authority shall monitor the correct application of the provisions of this measure and its annexes pursuant to Article 13-bis of Decree-Law No. 123/2023, converted, with amendments, by Law No. 159/2023 and subsequent amendments and additions.

This provision, including **Annexes A, B, and C**, is published on the Authority's website. *website* of the Authority.

This measure may be challenged before the Regional Administrative Court of Lazio within 60 days of its publication.

Rome, April 8, 2025

THE PRESIDENT
Giacomo Lasorella

THE REPORTING COMMISSIONER
Laura Aria

Certification of compliance with the resolution
THE SECRETARY GENERAL
Giovanni Santella

AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

Annex A to Resolution No. 96/25/CONS

TECHNICAL AND PROCESSING METHODS FOR VERIFYING THE AGE OF USERS FOR THE PURPOSE OFACCESS TO CERTAIN SERVICES PROVIDED BY WEBSITE OPERATORS AND VIDEO SHARING PLATFORMS THAT DISTRIBUTE PORNOGRAPHIC IMAGES AND VIDEOS IN ITALY, PURSUANT TO ARTICLE 13 BIS OF DECREE LAW NO. 123 OF SEPTEMBER 5, 2023, CONVERTED WITH AMENDMENTS BY LAW NO. 159 OF NOVEMBER 13, 2023

This measure specifies the technical and procedural methods that certain website operators and video sharing platforms that disseminate pornographic images and videos in Italy are required to adopt to guarantee that users are of legal age.

The purpose of the measure is not to certify technical solutions, but to establish a framework of minimum technical requirements, in accordance with the European legal framework on online services, with the specific aim of protecting minors online from pornographic content that could harm their health and physical, mental, and moral development.

The measure may be reviewed and updated to take account of the state of the art and, in particular, to ensure full compliance with the guidelines adopted by the European Commission pursuant to Article 28 of Regulation (EU) 2022/2065. Therefore, this measure constitutes a transitional solution as indicated in Article 4 of this measure.

Art. 1

IDENTIFICATION OF ENTITIES THAT MAKE PORNOGRAPHIC CONTENT AVAILABLE TO THE PUBLIC AND SCOPE OF APPLICATION OF THE TECHNICAL AND PROCESSING METHODS FOR VERIFYING THE AGE OF USERS

1. This measure, adopted in implementation of Article 13-bis, paragraph 3, of the Decree, applies to operators of websites and video-sharing platforms that disseminate pornographic images and videos in Italy, whether established in Italy or in another Member State. These entities are identified in a list compiled and updated by the Authority and communicated by the latter to the European Commission.

2. In order to establish whether content disseminated by a provider established in another Member State is directed at the Italian public, at least one of the following criteria must be met:

a) the *predominant* use of the Italian language within the online service, to be assessed in relation to the presence of textual elements in Italian in the user interface, as well as the availability of a multilingual function that includes Italian;

b) the online service reaching a significant average number of unique monthly users in Italy based on data provided by bodies that are highly representative of the entire sector in question, also in light of multimedia convergence processes, whose organization also complies with the principles of impartiality, autonomy, and independence;

c) the achievement by the video sharing platform service provider of revenues generated in Italy, even if accounted for in the financial statements of companies based abroad. These services are identified in a list compiled and updated by the Authority, which also communicates it to the European Commission.

d) the service is also promoted or marketed to Italian users;

e) the service has a domain in Italy or provides a contact address and/or telephone number in Italy.

3. Where the conditions set out in paragraph 4 of Article 3 of Directive 2000/31/EC are met, the scope of application referred to in paragraph 1 is also extended to website operators and video-sharing platforms that disseminate pornographic images and videos in Italy, established in another Member State, identified on a case-by-case basis by the Authority in accordance with European legislation and the procedure laid down in Article 3(4) and (5).

4. The Authority considers that the technical and procedural methods for verifying the age of users adopted in this provision are highly recommended, as they are effective, appropriate, proportionate, and functional, for their use by parties other than those indicated in the list referred to in paragraph 1 and with reference to additional types of content, in addition to pornographic content, which could nevertheless harm the physical, mental, or moral development of minors, such as the categories provided for in Resolution 9/23/CONS. mental, or moral development of minors, such as the categories provided for in Resolution 9/23/CONS.

Art. 2

DEFINITIONS

Decree: Decree-Law 123/2023 as converted by Law No. 159 of November 13, 2023.

Age assurance (hereinafter also referred to as ***Age assurance*****)** refers to the set of methods, systems, and processes used to determine an individual's age or age range at various levels of confidence or certainty. The three main categories of age assurance methods are **self-declaration, age verification, and age estimation**.

Self-declaration refers to the set of processes in which a user enters a date or selects a box on a form, including online, to declare that they are above/below a certain age, without providing any other evidence.

Age estimation refers to methods that determine that, with a certain probability, a user is of a certain age, falls within a certain age range, or is above or below a certain age. Age estimation methods include automated analysis of behavioral and environmental data, comparing how a user interacts with a device or with other users of the same age, metrics derived from body movement analysis, facial recognition, or analysis of skills or knowledge. In the methods used for estimation

Age verification also includes those carried out using algorithms and artificial intelligence-based technologies.

Age verification refers to systems based on rigid (physical) identifiers and/or verified sources of identification, which provide a high degree of certainty in determining a user's age.

Proof of age: a physical object (e.g., scratch card) or digital object (e.g., electronic document, file, alphanumeric string, electronic transaction, etc.) that allows the age of the user who uses it to be established on the basis of codified processes and protocols recognized by the parties.

Performance indicators: qualitative and quantitative parameters that allow the effectiveness of an *age assurance* system to be measured in terms of error containment in age determination, both in a test environment and in real operating conditions. The degree of effectiveness can be determined on the basis of specific indicators such as, for example, in the case of estimation-based systems, *the average error*, the *standard deviation*, the *false OK* rate, i.e., the *false positive* rate, in allowing access (understood as the probability that the system will allow access to content prohibited to minors). Another performance indicator used in some studies is *the mean absolute error (*a measure of the average difference between actual and predicted age), which must fall within acceptable tolerances.

Art. 3

REQUIREMENTS, TECHNICAL SPECIFICATIONS, AND PERFORMANCE INDICATORS OF *AGE ASSURANCE* SYSTEMS

1. The Authority adopts a technologically neutral approach, which leaves those responsible for implementing *age assurance* processes, identified in accordance with Article 1, reasonable freedom of assessment and choice, while establishing the relevant principles and requirements.

2. In view of the results of the public consultation and considering the opinion of the Data Protection Authority, in light of the analyses carried out, including at European level, the Authority establishes that a functional system for providing "Age Assurance" must comply with the **requirements and process and system specifications** described below.

i. **Proportionality:**

- This is a general, primary requirement that refers to the search for the right balance between the means used to achieve the set objective, in this case age verification, and its impact on the limitation of individuals' rights. The subjects referred to in Article 1 of this provision must use a tool that is as non-invasive as possible to achieve the set objective.
- Based on the principle of *accountability* referred to in Articles 5(2) and 24 of Regulation (EU) 20761679 ('GDPR'), it is appropriate for the subjects referred to in Article 1 to choose the age verification tools to be implemented in their service and to demonstrate the effectiveness of the tool used in accordance with the principles and requirements set by the Authority, as well as the compliance of the tool with data protection principles and rules, in particular that of proportionality. In this context, the document also considers the impact of the tool used on "individual rights" to be considered as fundamental rights and freedoms.

ii. **Protection of personal data:**

- The *age assurance* systems implemented must comply with the data protection rules and principles established by Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 - GDPR (data minimization, accuracy, storage limitation, etc.). The methods chosen for age verification must, in particular, comply with the principle of data minimization (Article 5 of the GDPR) and the principles of *data protection by design and by default (*Article 25 of the GDPR).
- Age verification processes involve the processing and management of personal data such as, for example, data contained in identity documents, the user's photograph, credit card holder information, etc. Therefore, in order to ensure the protection of users' privacy, the entities referred to in Article 1 of this provision that implement age verification processes must ensure that the processing of personal data complies with the obligations set out in the GDPR, providing appropriate information to users and ensuring that only personal data necessary for the purpose is collected.
- The logic of *parental control*, referred to in Resolution No. 9/23/CONS, which limits access to content through network and application filtering tools, restricts access to sensitive content without requiring the provision of sensitive data.
- The subjects referred to in Article 1 of this provision and third parties involved in the age verification process and related processes (e.g., system maintenance, service management or billing, etc.) must not carry out any profiling of users and, in particular, the age verification mechanisms implemented must not allow the subjects concerned to collect the identity, age, date of birth, or other information of users. etc.) must not carry out any profiling of users and, in particular, the age verification mechanisms implemented must not allow the parties concerned to collect the identity, age, date of birth, or other personal information of users.
- The Authority does not consider systems based on the following to be compliant with privacy requirements:
  - direct collection of identity documents by the publisher of the pornographic website;
  - age estimation based on the Internet user's browsing history on the web;
  - processing of biometric data for the purpose of identifying or authenticating a natural person (e.g., comparing, using facial recognition technology, a photograph on an identity document with a self-portrait or *selfie*).

Having regard to the opinion of the Data Protection Authority and the related considerations regarding the possible use of digital IDs provided in the public sphere, within the scope of possible solutions to be implemented and without prejudice to the need to preserve the freedom of assessment and choice of technology by the subjects referred to in Article 1 of this provision, the following is stated.

The use of public databases or an authentication system could theoretically comply with the technical and procedural methods indicated herein only on condition that its operation did not require the recording of uses on the servers of state bodies and private companies, as it is not permitted **to make available to such entities a list of links of a purely private nature and presumed sexual orientations.**

As illustrated in section I.8 of Annex B to this provision, the SPID system, for example, does not appear to be **fully compliant with the AGCOM technical specifications indicated below** for the purposes of implementing the provisions of Article *13-bis* of Law No. 123 of November 13, 2023

(essentially in the part where the so-called double anonymity is required), when the *Service Provider's* authentication request, which contains the domain name of the visited site, is transferred *to the Identity Provider*. In fact, this SPID authentication system allows *the Identity Provider* to know the particular site/platform visited by the user, and it cannot be ruled out that this information is stored within the *Identity Provider's* systems[1].

With regard to the level of protection of personal data appropriate to the risk and, in general, ensuring that the verification and authentication process complies with personal data protection legislation, it is worth highlighting the usefulness of the security levels offered by digital identity managers, who, it should be remembered, are themselves third parties (both in relation to the regulated entity and in relation to 'state bodies' and managers of 'public databases') and in possession of certain subjective and objective requirements established by sector regulations, selected on the basis of specific qualification procedures and subject to supervision by the Agency for Digital Italy (AGID)[2].

It should therefore be noted that a public system makes it possible to quickly establish a set of certified *Identity Providers* and a network of connections and agreements (based on existing regulatory obligations) capable of providing the user, and through them the platform, with so-called proof of age.

This applies both to age verification methods linked to age verification systems not based on applications installed on the user's terminal and to those based on applications installed on the user's terminal (so-called *digital wallets*), without prejudice to the need to preserve the user's freedom of choice regarding the use of one or the other system, also considering the potential invasiveness of installing certain apps on their personal device.

Therefore, only where the requirements set out in the following section on double anonymity (protection of personal data vis-à-vis the website/platform and lack of knowledge of the website visited/platform by *the Identity Provider*) are met, does the Authority consider that public systems can be used.

Minimum requirements applicable to all age verification systems

The following criteria constitute a minimum set of requirements applicable to all age verification systems covered by this provision.

Independence of the age verification system provider from services that disseminate pornographic content

The provider of age verification systems must be legally and technically independent from website operators and video sharing platforms that disseminate pornographic images and videos in Italy covered by this provision; it must also ensure that the targeted parties disseminating pornographic content do not, under any circumstances, have access to the data used to verify the user's age.

---

[1] By way of example, the *SPID Single Sign On - SP initiated redirect* authentication method allows the decoupling of *user-service_provider* and *user-identity_provider* interactions. In this way, the *Service_provider* does not communicate directly with *the identity_provider* for authentication purposes, but through the *User_agent.*

However, the technical documentation for *SPID's Single Sign On* mode (available at https://docs.italia.it/italia/spid/spid-regole-tecniche/it/stabile/single-sign-on.html#example-of-authnrequest), however, provides for the exchange of messages containing **metadata** from *the Service_provider* to *the User_agent* and *from the Identity_provider* to *the User_agent*, including the URL of the Service Provider, i.e., the address of the site visited by the user, to which the response message to the authentication request should be sent.

[2] For example, for the "certification" component alone, the SPID system has been based, since its inception, on a process of accreditation and supervision of the entities that carry it out.

Confidentiality with regard to services that disseminate pornographic content

Personal data that allows the user to verify their age with a service covered by this regulation must not be processed.

In particular, the implementation of age verification solutions must not allow the targeted entities concerned to collect the identity, age, date of birth, or other personal information of such users.

Confidentiality regarding providers that generate proof of age

Where the age verification system does not allow the user to obtain a digital identity or reusable proof of age, the personal data provided by the user to obtain age verification should not be retained by the age verification service provider. Furthermore, this type of system should not require the collection of official identity documents.

Confidentiality towards any other third parties involved in the age verification process

Where third parties other than age verification providers are involved in the age verification process, for example for the management of the verification or billing of the service, such third parties shall not retain the personal data of users of the system, except for the storage of the verification at the request of the user.

Enhanced confidentiality for services that disseminate pornographic content

An age verification system that uses "double anonymity," i.e., based on the intervention of an independent third party (section iii below), must not allow the targeted parties concerned to recognize a user who has already used the system on the basis of the data generated by the age verification process.

The use of age verification systems that use "double anonymity" must not allow the aforementioned services to know or deduce the source or method of obtaining age evidence involved in a user's age verification process.

An age verification system that complies with "double anonymity" must not allow the aforementioned services to recognize that two pieces of evidence of age come from the same source of age evidence.

Enhanced confidentiality for individuals who provide proof of age

The *enhanced confidentiality* requirement, which is in addition to the *confidentiality* requirement[3]above, provides for an age verification system that uses the "double anonymity" model, whereby those providing proof of age must not be allowed to know for which service the age verification is being performed. In particular, in the age verification process using "double anonymity," individuals providing proof of age must not be given information about the website/platform the user wants to access.

Greater confidentiality towards any other third parties involved in the age verification process

An age verification system that uses "double anonymity" must not allow any other third party involved in the process to recognize a user who has already used the system. Ad

[3] It should be noted that the *confidentiality* requirement, with regard to services that disseminate pornographic content, stipulates that personal data enabling users to verify their age with a service covered by this Regulation must not be processed. In particular, the implementation of age verification solutions must not allow the services covered by the regulation to collect the identity, age, date of birth, or other personal information of such users.

For example, a third party that ensures the transmission of proof of age or certifies its validity must not be able to know whether it has already processed proof from the same user.

iii. **Intervention by independent third parties:**

In general, the Authority considers an age verification system that involves two logically separate steps to be compliant with these technical specifications: identification and authentication of the person identified for each session of use of the regulated service.

AGE VERIFICATION SYSTEMS NOT BASED ON APPLICATIONS INSTALLED ON THE USER'S TERMINAL

- In this case, an age verification process capable of providing the necessary level of personal data protection must be divided into three distinct phases:

  - firstly, the issuance of 'proof of age', with a certain level of confidence, **following identification.** This proof may be issued by various entities that know the internet user, whether they are service providers specialising in the provision of **digital identity,** or an organisation or entity that has identified the internet user in another context. **The entity providing the "proof of age" is not aware of the use that the user will make of it.**

    The Authority considers it appropriate that website operators and video sharing platforms that disseminate pornographic images and videos in Italy do not carry out age verification operations themselves, but rather rely on independently verified third-party solutions. Therefore, the entity providing an *age assurance* service, according to the above process, must be legally and technically independent from the content provider (website or video sharing platform) for the following reasons.

    The use of a trusted (or certified) independent third party avoids the direct transmission of user identification data to the website or platform offering pornographic content. Entrusting these functions to different parties makes it possible to ensure maximum protection of personal data thanks to a process that guarantees the separation of the actors, i.e., between the user, the content provider, and the entity that certifies the user's age. The Authority considers it necessary that providers of age verification, unless already subject to regulatory obligations to identify users, be subject to third-party assessment (i.e., that they be certified to some extent). As mentioned above, in the case of public systems, digital identity managers are themselves "third parties" (both with regard to the regulated entity and with regard to 'state bodies' and managers of 'public databases') and meet certain subjective and objective requirements established by sector regulations, as well as being selected on the basis of specific qualification procedures and supervised by the Agency for Digital Italy (AGID).

  - Secondly, this certified proof of age must be provided to the user or directly to the website or platform visited so that they can decide whether or not to grant access to the requested content. The website or platform provider does not obtain any data on the user's identity. If the person providing the "proof of age" sends it directly to the website or platform, this is not considered compliant, as it means that the same person issuing the proof of age will be aware of the specific website or platform visited by the user. **Conversely, the model proposed by the Authority, which provides for the communication of proof of age only to the user**

who will then present it to the site or platform visited, provides the maximum guarantee for data protection. In fact, in this case, the person issuing the proof of age does not know the particular site or platform that the user wants to visit, and at the same time, the site or platform visited will not know the user's identity. Furthermore, if the person providing the 'proof of age' is a private individual who is not already subject to specific legal obligations regarding identification, such as an 'age assurance' service provider, it is advisable that they be certified by a specific Authority in order to have guarantees regarding the identification system used.

- A third step, implemented by the website or platform visited by the user, consists of analyzing the proof of age presented and granting or denying access to the requested content (**authentication**).

- Below is an example of the above process:

1) The entity providing the "proof of age," such as a bank, telephone operator, public body, or private entity (including a merchant) where the user has been reliably identified for other services or for the purpose of accessing adult content and services, knows the identity of the internet user but does not know which website/online service they are visiting.

2) At the user's request, the third party provides "proof of age" (a kind of certification) which is delivered to the user (in the case of scratch cards, for example) or sent to the user (in the case of an electronic process). This "proof of age" does not contain any data that identifies the user or allows the user to be traced. For example, in the case of electronic provision of "proof of age," it is possible to envisage systems that use public and private key encryption to manage certification and verification as described below([4]) :

   a) to access the content, the website or video platform requires the user to verify their age and sends an object (e.g., a file or alphanumeric string) called "age to be proven.**" This object does not contain any reference to the website, video sharing platform, or content that the user wants to access.**

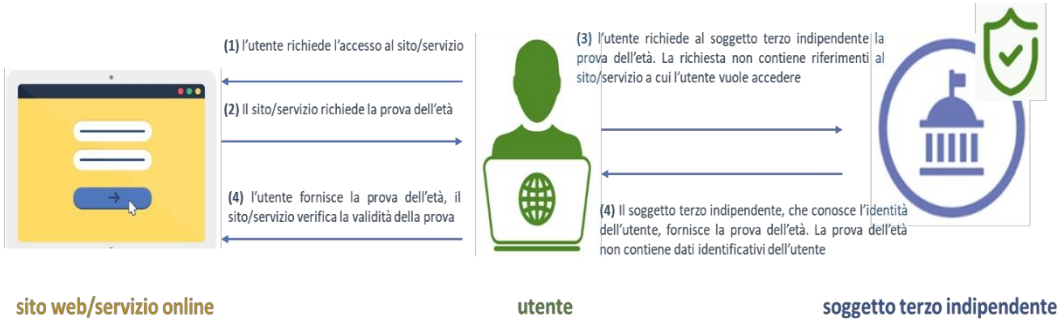
   b) The user asks the third party to provide proof of age, certifying the object called "age to be proven." The third party certifies the "age to be proven" object by encrypting it with a private key, thus generating a new object called "proof of age." This certification does not contain any data on the user's identity or age.

   c) The user sends the "proof of age" to the site or platform they wish to access. The site or platform applies public key decryption to the "proof of age" to retrieve the content of the object, then verifies that this content is valid and consistent with that initially sent to the user and carries out the necessary checks to avoid the risk of reuse or fraudulent creation of certifications.

[4] Asymmetric encryption is a form of cryptographic system in which two different keys perform encryption and decryption. These two keys are the public key and the private key. Each participant has a pair of public and private keys. The public key is accessible to all other participants. However, the private key is only accessible to its owner. The sender uses the recipient's public key to encrypt the message. When a message reaches the recipient, they use their private key to decrypt the message.

This application requires the existence of a Certification Authority that generates, shares, revokes, and manages certificates and encryption keys.

3) The website operator or video sharing platform that disseminates pornographic images and videos in Italy obtains proof of the user's age and, while necessarily knowing the specific online content accessed by the user, has no information about their identity.



- The Authority emphasizes the importance that the "proof of age" contains only information about the user's age of majority and, therefore, does not include references to their identity or chronological age.

AGE ASSURANCE SYSTEMS BASED ON THE USE OF APPLICATIONS

- The third party providing proof of age makes an app available to the user for the certification and generation of "proof of age" (e.g.**, digital identity wallet app, or digital identity management app,** etc.). In this case, with reference to point (a) above, the "age to be proven" object, presented by the website/video *sharing* platform to the user, can also be obtained via a QR Code([5]) ·By scanning the QR Code with their smartphone camera, the user accesses, via a link, a service (present on the platform/website) dedicated to authentication and will use the APP to send the "proof of age" directly from their device and without the intervention of any external web service, so that the confidentiality of the information relating to the site/platform/content visited is guaranteed and that this information is not disclosed to external parties, but is managed exclusively within the user's device.

- Pursuant to Article 12-ter, paragraph 3, of the "Regulation of the European Parliament and of the Council amending Regulation (EU) No. 910/2014 as regards the establishment of a framework for a European digital identity," very large *online* platforms, as defined by the DSA, which require users to authenticate themselves in order to access online services, must **also accept the use of European digital identity wallets (EU digital wallets),** strictly on the voluntary request of the user, including with regard to

[5]QR Code is short for "Quick Response Code," which is a matrix barcode that responds quickly. It is a symbol that returns data and information to the user whenever it is scanned by a smartphone camera.

minimum attributes required for the specific online service for which authentication is required, such as proof of age.

iv. **Security:**

- The *age assurance* system must take into account possible cyber attacks and provide for sufficient cybersecurity measures to mitigate risks (GDPR, proposed Cyber Resilience Act - CRA) and prevent attempts at circumvention.

  All processes are more or less vulnerable to cyber attacks or attempts by minors themselves to circumvent the verification system. *Age assurance* systems should identify possible vulnerabilities in the process, such as:

  (a) The accuracy, reliability, and risk of fraud of the data source, including consideration of the risks associated with inferring or deriving data from other sources used for other purposes;

  (b) The possibility of an attack on the system; systems should be put in place to reduce attempts at circumvention by bots or automated processes; for online age assessment, system developers should assess the risk that a non-human process could be used for a system-level attack.

  (c) The possibility for an individual to circumvent the system; for example, a minor could present an image of an identity document that does not belong to them, a forged document (e.g., a fake driver's license, a forged passport, or a forged registration in a database), or use still images or videos in cases of facial recognition. it is therefore necessary to provide techniques for establishing the liveness of an individual. A system for detecting so-called liveness, for example as defined by ISO/IEC 30107, therefore becomes important;

  (d) The possibility of collusion or complicity between parties (including between minors and adults);

  Other types of attacks may occur through the acquisition of biometric data directly from a person, online, or through existing databases, using them for biometric *spoofing* (e.g., a person's face image or video on a tablet or a fake silicone or gelatin fingerprint) to a biometric sensor;

  With regard to the devices currently available on the market, several regulators point out that all the solutions currently on offer can be circumvented in some way. For example, the use of a VPN, which was created to ensure the security of users when using the Internet, can at the same time allow a minor to circumvent an age verification system. The entity required by law to implement the age verification system for access to content must not promote or refer to any mechanism for circumventing *age assurance* systems.

v. **Accuracy and effectiveness:**

- The *age assurance* system must be effective in terms of limiting errors in age determination both in a test environment and in real operating conditions. The degree of effectiveness can be determined on the basis of certain performance indicators such as, for example, in the case of estimation-based systems, *the mean error*, the *standard deviation*, the false positive rate, i.e., the rate of false positives, in allowing access (understood as the probability that the system will allow access to content prohibited to minors).

, the *false positive* rate, i.e., the rate of *false positives*, in allowing access (understood as the probability that the system will allow access to content prohibited to minors).

Another performance indicator used in some studies is *the mean absolute error* (a measure of the average difference between actual and predicted age), which must fall within acceptable tolerances.

The age verification mechanism must correctly determine a user's age in real, unexpected, or actual operating conditions, ensuring adequate performance compared to data obtained in the laboratory. For example, age verification mechanisms must ensure adequate performance under conditions that alter the quality or characteristics of the input, such as poor lighting, blurring, brightness, contrast, or user positioning in the image (for methods based on a photographic image of the face, or on a photo ID, etc.) or even camera resolution.

The age verification mechanism must provide performance that does not vary over time. This could be the case with AI-based systems, where population data and demographics may change over time, leading to a greater degree of variance in the age verification mechanism. This is because the data on which the mechanism was trained becomes less representative of the population that actually uses it. This requires continuous monitoring of the accuracy of the mechanism used, making the necessary corrections.

- Age verification based on self-declaration is not considered an effective method for correctly determining a user's age.
- The age verification system must be neutral or independent of the device or operating system used by the user.
- Website operators and video sharing platforms that distribute pornographic images and videos in Italy must ensure that no user accesses pornographic content until they have proven that they are of legal age, i.e., until the age assurance process has been completed.
- The *age assurance* process must take place each time a specific website or *video sharing* platform that disseminates pornographic content is accessed. After the service has been interrupted, a new age verification must be triggered in the event of renewed access to pornographic content.
- The validity of an age verification must therefore cease when the user exits a given service, i.e., when the session ends, when the user exits the browser, or when the operating system goes into standby mode, and in any case after a period of 45 minutes of actual inactivity in order to prevent the viewing of pornographic content without further verification in the case of a device shared between an adult and a minor.

vi. **Functionality, accessibility, ease of use, and no obstacle to accessing content on the Internet:**

- Age verification systems must be easy to use and based on the abilities and characteristics of minors. Age verification should not restrict access to the Internet but rather promote it, without creating unnecessary obstacles to the use of services and content.

- Age verification systems must be accessible. Accessibility means that the age verification system must be easy to use for all users, regardless of their characteristics (age, gender, ethnicity, language, etc.), their level of computer literacy, or whether they belong to a particular group (e.g., users with disabilities). Therefore, website operators and video-sharing platforms that distribute pornographic images and videos in Italy must ensure that the system implemented is easy to use and does not unduly prevent adults from accessing legal content. This could happen, for example, if the mechanism is too difficult to use, causing users to abandon the verification process and therefore the website or video-sharing platform. In addition, the potential impact that the age verification system or systems implemented may have on use by users with disabilities must be assessed, ensuring, for example, that screen readers can be used to successfully complete the verification process.
- It would be advisable to make more age verification solutions available, allowing users to choose which one to use based on their characteristics and needs.
- Age verification should not require the creation of a user account for the service offered by the regulated entity. Furthermore, proof of age cannot be stored in a user account on that service. In any case, the age verification requirement applies to every access, with or without a user account.

vii. **Inclusiveness and non-discrimination:**

- Non-discrimination is one of the four general principles of the UN CRC. Differences between children in terms of language, ability, socioeconomic status, etc. should be taken into account during the age verification process.
- This criterion refers to the ability of the age verification system to prevent or minimize unintended bias and discriminatory outcomes for users. Therefore, where applicable, website operators and video-sharing platforms that disseminate pornographic images and videos in Italy must ensure that age verification mechanisms have been trained on different datasets in order to avoid discriminatory results for certain groups of users, for example, a lower degree of technical accuracy for users of a certain ethnicity when the mechanism is based on facial age estimation, or even to prevent underage users from being mistakenly identified as adults, or adult users from being mistakenly identified as minors.

viii. **Training and information:**

- The Authority highlights the importance of informing and raising awareness among minors, parents, educational community staff, and youth management about good IT practices and the risks associated with the Internet. Activities related to the implementation of parental controls have highlighted the centrality of this aspect.

x. **Complaint management:**

- The *age assurance* service provider must provide at least one channel for promptly receiving and handling complaints in the event of incorrect age decisions.

xi. **Monitoring:**

- In order to ensure a high level of protection for minors, the Authority will assess, on a case-by-case basis and in concrete terms, the technical solutions for age verification once they have been implemented and are operating in real conditions. The entities referred to in Article 1 are required to ensure that the solutions implemented are systematically capable of meeting the requirements set out in this provision, adapting their operating principles and parameters where necessary.

xii. Supervision and cooperation:

- Without prejudice to the provisions of Articles 1 and 4 of this measure, the Authority shall cooperate closely with the Commission and with the national coordinators for digital services designated in the other Member States, on the basis of the country of origin principle, and shall provide mutual assistance for the consistent and efficient application of this measure, including through the exchange of information and any other necessary measures, activating the relevant cooperation procedures between Member States through the IMI system, also making use of the guidance provided by *the Memorandum of Understanding.*

Art. 4

ENTRY INTO FORCE AND REVIEW CLAUSE

1. Pursuant to Article 13-bis of the Decree, website operators and video sharing platforms that disseminate pornographic images and videos in Italy shall implement effective systems for verifying the age of users in accordance with the requirements set out herein within six months of the date of publication of this measure.

2. Without prejudice to the conditions and procedures set out in Article 1, paragraph 3, the provisions of this measure shall also apply to website operators and video-sharing platforms that disseminate pornographic images and videos in Italy, regardless of the Member State of establishment, three months after the publication of the list referred to in Article 1 of this measure.

3. From the date of entry into force of the guidelines adopted pursuant to Article 28 of Regulation (EU) 2022/2065, the Authority undertakes, where necessary, to amend and adapt this measure to the European legislation that has come into force with reference to entities established in other Member States.

AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

Annex B to Resolution No. 96/25/CONS

EUROPEAN AND NATIONAL FRAMEWORK ON TECHNICAL AND PROCESSING METHODS FOR VERIFYING THE AGE OF USERS

Summary

I. Introduction

Online age verification methods for minors

For over two decades, a limited range of *online* age verification methods has been available to protect minors from accessing *online* content that is unsuitable for their age. However, protecting this group of users in their *online* activities is becoming an increasingly vital issue in today's social context.

As reported in the February 2023 report "*Online age verification methods for* children" by *the European Parliamentary Research Service* (EPRS), many countries are introducing laws and/or codes of conduct to address this issue. Efforts are also intensifying at EU level through the adoption of a code of conduct, which is currently under review. The identification of measures to verify the age of users presents, as explained in more detail below, a number of complex issues, not least in the areas of privacy protection, monitoring, and the need to improve the digital skills of parents and children.

According to the aforementioned document, it has been observed that, partly as a result of the coronavirus pandemic, minors have become accustomed to spending more time *online*. Global estimates reveal that one in three minors is an Internet user and that one in three Internet users is under the age of 18. In the EU, most minors use their smartphones every day, almost twice as many as 10 years ago. In most cases, however, the *online* environments they access were not originally designed for them (for example, in some cases, *social media* requires a minimum age of 13 for its users). In general, digital services do not use adequate methods of age verification or parental consent.

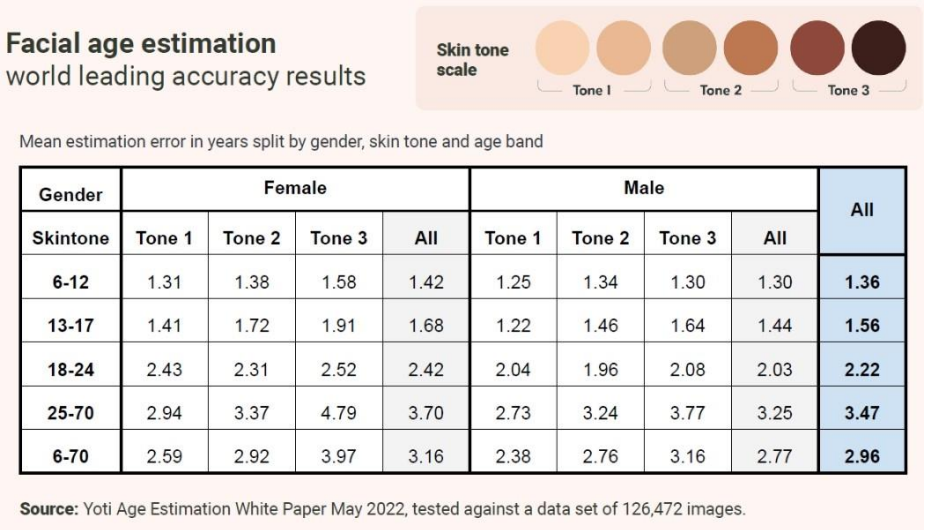
Online age verification methods are becoming increasingly diverse. Below is a list of those considered most common according to the EPRS report.

A. Self-declaration: methods that require, for example, the user to enter their date of birth without further evidence to confirm this information, or that ask the user to tick a box on an online form to confirm that they are at least 18 years old. It has been shown that this method, the most common of all, can be easily circumvented. The most common examples include self-declaration of one's date of birth.

B. Credit card: here, users are required to verify the validity of their cards by entering their credit card details or, in some cases, by making a bank or card payment of €0.01. The *payment provider* provides confirmation of legal age. This method is mainly used by e-commerce sites and apps that sell adult products such as alcohol or adult content. Beyond the inherent risk of *phishing*, this document considers that it is not possible to ascertain that the person using the card is the legitimate holder; furthermore, the age for owning a credit card varies from country to country.

C. Biometrics: This method relies on artificial intelligence (AI), which powers the use of biometric technologies, including facial recognition applications. These systems can be used to analyze facial features using a *selfie* to verify that the person requesting access is over 18 years of age. However, this approach has a margin of error; moreover, minors could use the face of an adult to gain unauthorized access. Authentication methods using biometrics raise *privacy* concerns due to excessive data processing and profiling.

Some providers consider it an instantaneous process—scalable to tens of millions of units per day—where no images are stored. Below is a table containing, based on analyses carried out by some analysts, an indication of performance in terms of statistical error of estimation.



Mean estimation error in years split by gender, skin tone and age band

Gender	Female				Male				All
Skintone	Tone 1	Tone 2	Tone 3	All	Tone 1	Tone 2	Tone 3	All	
6-12	1.31	1.38	1.58	1.42	1.25	1.34	1.30	1.30	**1.36**
13-17	1.41	1.72	1.91	1.68	1.22	1.46	1.64	1.44	**1.56**
18-24	2.43	2.31	2.52	2.42	2.04	1.96	2.08	2.03	**2.22**
25-70	2.94	3.37	4.79	3.70	2.73	3.24	3.77	3.25	**3.47**
6-70	2.59	2.92	3.97	3.16	2.38	2.76	3.16	2.77	**2.96**

Source: Yoti Age Estimation White Paper May 2022, tested against a data set of 126,472 images.

D. Analysis of *online* usage patterns (online behavior analysis): these are age verification systems based on inference, such as importing an individual's Internet browsing history or analyzing their "maturity" through a questionnaire or user-generated online content or purchases.

E. *Offline* verification: this is carried out using so-called 'scratch cards', i.e. by acquiring an ID certifying that the person is of legal age, or *offline* age checks *in situ* using documents. This is a so-called *one-time* verification.

F. *Online* verification: this is carried out through document checks. For example, in the case of photo ID matching, the photograph on the identity document uploaded by the user, which also includes their date of birth, is compared with a photograph of the user taken when the document was uploaded to verify that it is the same person.

G. Parental consent: Some apps and services require parental consent to register a minor for a digital service. However, parental authority is rarely fully verified. Proving parental authority/guardianship may involve checking traditional identity documents and family records.

H. *Vouching*: Users other than parents are asked to provide *online* confirmation that a child requesting *online* access is of the right age.

I. Digital identification (digital ID): This method relies on tools provided by state authorities to verify people's identity and age before granting them access to digital services (e.g., SPID).

J. *Digital identity wallet*: The digital identity wallet allows users to prove their identity when necessary to access *online* services, share digital documents, or simply prove a specific personal attribute, such as age, without revealing their full name or other personal data. Within the EU, there is a proposal to create a European digital identity wallet[1].

K. Age verification via a specific app: these are applic~~ations that are mostly linked to the prior~~ acquisition of an identity document and a selfie. In some applications available on the market, users provide a copy of an identity document and

[1] https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-toolbox

take a biometric selfie to create their own reusable digital ID. Once verified, access is granted after scanning a QR code.

L. Models based **on mobile phone numbers** and comparison with data held by the telephone operator can be added to the above list. Others carry out verification by **email** or even by **voice analysis**.

M. **Open banking:** this method uses certain information that a credit institution has recorded about a user's age, with the user's consent. Confirmation of whether or not the user is over 18 is shared with the website/service provider requesting verification of the user's age. The user's personal data, including their date of birth, is not shared with the website/service provider.

Only recently, based on research, have social platforms begun to implement age verification measures.

A. In 2022, **Instagram** began testing a tool to ensure that users are the age they claim to be; in some cases, it has also begun using biometric technology for facial analysis.

B. **YouTube** launched an app dedicated to minors and introduced new data practices.

C. **Meta** created Messenger Kids on Facebook, which allows minors to connect only with contacts approved by their parents.

D. **TikTok** does not have an age verification method but may ban accounts after registration.

E. Twitter verifies parental consent by requesting documentation (ID card/birth certificate, etc.). Twitter states that documents are treated confidentially and are deleted after verification.

F. E-commerce sites that sell adult products and services such as gambling, alcohol, or pornography have a wide range of age verification methods such as credit cards, scratch cards, and biometric data.

Based on the findings of the above report, a number of key challenges remain, of which the following three are particularly relevant:

A. Privacy/cybersecurity risks: Despite the widespread use of age verification methods in some sectors, there are still concerns that they pose privacy and cybersecurity risks. Given the sensitivity of the data collected by some age verification systems, **some suggest implementing third-party certification.** To date, there are no common EU guidelines on methods for determining age verification, and it has been found that minors can easily circumvent most solutions.

B. Content not sufficiently appealing to minors: Since apps and digital services for minors tend to offer a limited set of features, many prefer to lie about their age in order to use those designed for adults. This makes minors more vulnerable not only to privacy risks but also to security threats, such as online grooming or exposure to content inappropriate for their age. Usability for young users needs to be considered during the software design phase.

C. Better digital skills: Parents, children, and guardians need better digital skills and greater awareness of the risks involved.

At the regulatory level, the following picture emerges within the EU.

Before the adoption of the General Data Protection Regulation **(GDPR),** which came into force in 2018, there were no specific restrictions on the online processing of children's data in Europe. Article 8 of the GDPR introduces verification by data controllers of the age and parental consent of minors. Furthermore, recital (38) specifies that minors deserve specific protection with regard to their personal data, as they may be less aware of the risks, consequences, and safeguards involved, as well as their rights in relation to the processing of personal data. Such specific protection should, in particular, cover the use of children's personal data for marketing or profiling purposes and the collection of personal data relating to children when using services provided directly to a child. The **Audiovisual Media Services Directive (AVMSD)** requires the adoption of appropriate measures to protect children from harmful content online, including through age verification. In addition, the new European strategy for a better internet for children provides for an **EU code of conduct for age verification by 2024,** based on the new rules of the Digital Services Act (DSA) and in line with the AVMSD and the GDPR. A similar code already exists in other parts of the world, such as the United Kingdom and California.

In the context of **the EU eID proposal**, the **Commission intends to strengthen age verification methods through a robust certification and interoperability framework**. In addition, the **proposed regulation to combat online child sexual abuse** provides for improved online age verification. Also worth mentioning is the EU-co-funded **euCONSENT project**, which is developing an interoperable browser-based age verification method. The European Parliament has called for better age verification methods to protect children online on several occasions, including in its own-initiative report on consumer protection in online video games adopted in January 2023 and in its March 2021 resolution on children's rights in light *of the EU Strategy on the Rights of the Child.* Similarly, better age verification methods to protect minors online are part of the European Commission's proposal for a European Declaration on Digital Rights and Principles for the Digital Decade and the OECD Declaration on a Trustworthy, Sustainable and Inclusive Digital Future.

Further useful background information can be found in the document "***Consistent implementation and enforcement of the European framework for audiovisual media*** services," AVMS, prepared **by ERGA Subgroup 1**.

In fact, in 2023, ERGA Subgroup 1, which is responsible for implementing the above-mentioned Directive, conducted a comparative analysis of existing age verification mechanisms (AVMs), particularly for video-sharing platforms in the European Union (EU).

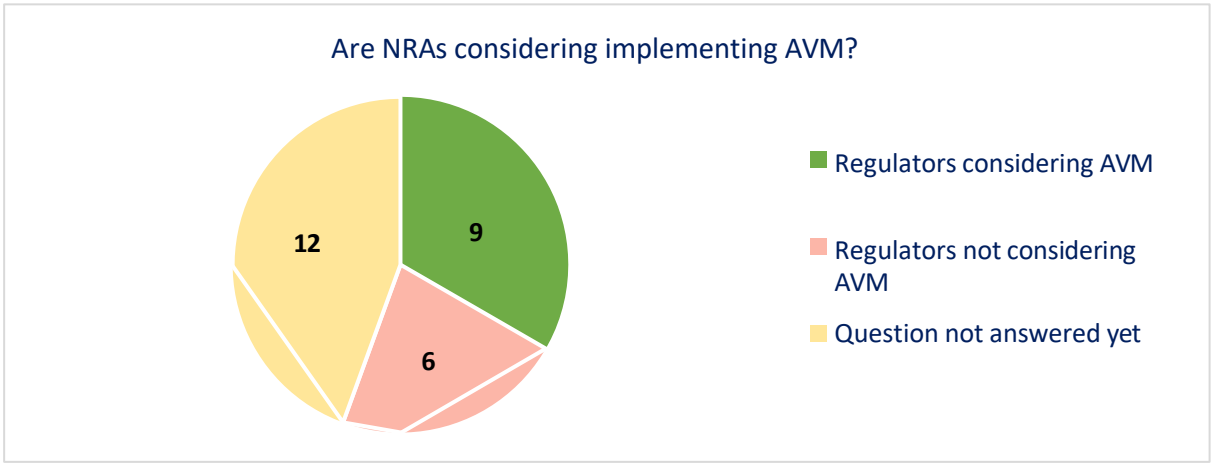
ERGA also recognizes that identifying and implementing efficient mechanisms to prevent children from accessing harmful content, and in particular pornographic content, raises a number of challenges, both in terms of efficiency (as some of these mechanisms can be easily circumvented) and privacy. The challenge for legislators and regulators is to strike the right balance between ensuring a high level of privacy for users, an efficient mechanism, and its widespread implementation by all stakeholders.

In order to collect data on this subject, on July 17, 2023, a questionnaire was sent to the countries participating in ERGA concerning the transposition of Articles 6(a) and 28-ter (paragraph 3, letter f) of the AVMS Directive and the national implementation of the AVM, with particular attention to minors' access to pornographic material. Twenty-seven NRAs responded, representing 25 EU Member States and one EFTA Member State.

Twenty-three NRAs responded that there are legal restrictions prohibiting minors from accessing pornographic content, regardless of the type of service (linear, non-linear, or online services).

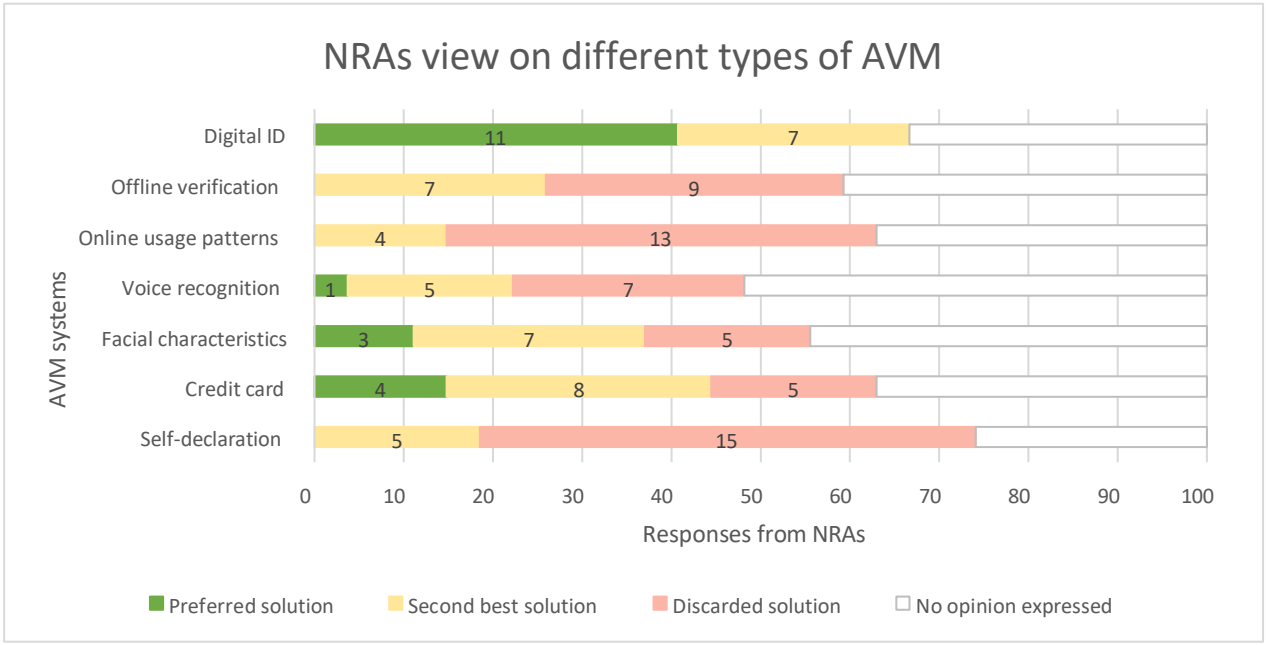
With particular regard to the implementation of age verification mechanisms in ERGA member states to restrict minors' access to pornographic content, 12 NRAs responded that they did not yet have a specific position.

Nine NRAs responded that AVM had been considered, while six NRAs responded that it had not.



In most countries where initiatives have been adopted (CZ, DE, DK, ES, FR, IT, LU, PL, PT), the mechanism adopted or soon to be adopted is provided for by law.

With regard to the technical solution, the following picture emerges in response to the question of which **solution** is **preferred by ERGA members for AVM:**



Age verification based on digital identity, such as the use of tools provided by the state to verify people's identities in general, **seems to be the preferred solution[2].**

Conversely, self-declaration is the least preferred solution among those proposed based on the responses, as 15 NRAs rejected it and 5 NRAs ranked it as the second best solution, with none ranking it as their preferred solution.

Online usage models **and offline verification** are also considered inadequate, and no NRA cites them as their preferred solution[3].

With regard to **credit card-based AVM**, 4 NRAs responded in favor, 5 NRAs were opposed, and 8 NRAs were not opposed but still encountered problems in this regard.

There is little consensus on methods based on facial feature analysis or voice recognition[4].

The ERGA report identifies **the following main challenges for AV systems:**

- the effectiveness of the system;

- data protection issues;

- ease of use and accessibility.

The ERGA report concludes that, although AVMs are not yet fully implemented (with the exception of self-declaration systems) in most Member States, many NRAs are addressing the issue with particular reference to the efficiency and security of the various systems. The intervention of an independent intermediary is an option being considered by many NRAs, reflecting concerns about privacy. In this regard, the **digital identity-based** solution seems to be the preferred option for most NRAs, although some are not entirely convinced. **Self-declaration is almost unanimously rejected** as an effective AVM.

Technical solutions available on the market

Systems developed by third parties, which provide age verification services to applicants, allow the following information to be obtained:

- whether the user's age exceeds the minimum requirement;
- the user's age.

Various methods are generally used, the most common of which are as follows:

1. Age estimation through facial recognition (biometrics)
2. Scanning of identity documents
3. App

[2] 11 NRAs (BE – VRM, BE – CSA, DE, EE, HR, LT, LU, LV, NL, SI, SK) ranked it as their preferred solution, 7 NRAs (AT, CZ, EL, FR, IT, PL, PT) as their second choice, and no NRAs responded by rejecting the solution.

[3] Online usage models have 13 responses (AT, BE – VRM, BE – CSAbe, CZ, EE, FR, LT, LU, NL, NO, PL, PT, SK) against and 4 responses (HR, IT, LV, SI) as second best; offline verification has 9 responses (BE – VRM, BE – CSA, EE, FR, LT, LU, LV, NL, PL) against and 7 responses (AT, CZ, HR, IT, PT, SI, SK) as second best.

[4] The first option received 3 responses (AT, DE, NL) in favor, 7 responses (HR, FR, IT, LV, LU, PL, SK) as second best opinions, and 5 responses (BE – VRM, BE – CSA, CZ, EE, LT) against. the second has 1 response (NL) in favor, 5 responses (AT, IT, LU, LV, SK) as second best and 7 responses (BE – VRM, BE – CSA, CZ, EE, HR, LT, PL) against.

4. Credit card
5. Mobile phone number
6. Comparison with data in certified databases.

1. Age estimation

The user is asked to take a selfie using their device's camera. This captures multiple images, one of which will be analyzed by the age estimation system based on Artificial Intelligence algorithms.

2. ID document scan

The user is asked to scan their identity document using their device's camera. The provider extracts the information from the identity document and verifies whether the age is above that required by the organization using the date of birth.

The user may also be asked to take a selfie using the device's camera. This is to verify that the ID document belongs to the user. The data acquired, such as the ID document and selfie, are stored in the data center. Once the session is complete, all personal information is deleted.

3. App

The user is asked to scan a QR code directly from the app, which performs the verification and sends the date of birth information to the site/platform. Before this step, the user must complete a one-time verification process with the app by uploading their ID document and a selfie.

4. Credit card

The user is asked to enter the credit card number, expiration date, postal code, and CV2 number.

The data is sent to the payment service provider and a small amount is retained to verify that the card is current and valid. Once the age has been verified, the amount is refunded.

5. Cell phone number

Users enter their name, date of birth, cell phone number, and address.

This data is sent to the operator. Users will receive a text message asking them to confirm their age by replying to the message. This serves to confirm that they are in possession of the mobile phone. The telephone service provider then confirms that the data entered on the website matches the data in the mobile service account, which is used to determine that the user is over 18 years of age.

6. Database check

You are asked to prove your age using your name, date of birth, and address.

This data is sent to a personal data certification agency to confirm that it is accurate and to obtain or confirm your date of birth.

Reusable age checks

To reduce the number of times online age verification is required, some providers develop an "age token" system. Age tokens function as digital proof of an age check and allow you to reuse the age check result for as long as the organization

allows it. You can save age tokens in an "age account." This allows you to access the organization's website, another browser, or another device without having to prove your age each time[5].

II. National regulatory framework

Italian law has dealt with the issue of age verification by recipients of services offered by online platforms in several provisions.

Legislative Decree No. 208 of November 8, 2021, *implementing Directive (EU) 2018/1808 of the European Parliament and of the Council of November 14, 2018, amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation, or administrative action in Member States concerning the single text for the provision of audiovisual media services in view of market developments" (*hereinafter TUSMA), as amended by Legislative Decree No. 50 of March 25, 2024, introduced, in Article 3, paragraph 1, letter c), into Italian law the definition of *a video-sharing platform service* as *"a service, as defined in Articles 56 and 57 of the Treaty on the Functioning of the European Union, where the main purpose of the service itself, a distinguishable section thereof, or an essential feature thereof is the provision of user-generated programs or videos intended for the general public, for which the video-sharing platform provider has no editorial responsibility, for the purpose of informing, entertain or educate via electronic communications networks within the meaning of Article 2(a) of Directive 2002/21/EC of the European Parliament and of the Council of July 12, 2002, and whose organization is determined by the video-sharing platform provider, including by means of automated means or algorithms, in particular by means of display, tagging, and sequencing."*

In addition, it has dedicated two specific provisions to the regulation of video-sharing platform services: Articles 41 and 42 of the TUSMA.

In particular, Article 41 provides the criteria for identifying providers of such services established or considered to be established in Italy.

Furthermore, this provision introduced into Italian law specific regulations aimed at providers of such services established in another Member State whose content is directed at the Italian public.

In this regard, paragraph 7 of Article 41 establishes that:

Without prejudice to Articles 14 to 17 of Legislative Decree No. 70 of April 9, 2003, and without prejudice to the provisions of the preceding paragraphs, the free movement of programs, user-generated videos, and audiovisual commercial communications conveyed by a video-sharing platform ***whose provider is established in another Member State and directed at the Italian public may be restricted,*** *by order of the Authority, in accordance with the procedure laid down in Article 5, paragraphs 2, 3, and 4 of Legislative Decree No. 70 of 2003, for the following purposes: a) the protection of minors from content that may harm their physical, mental, or moral development in accordance with Article 38, paragraph 1;*

Furthermore, pursuant to Article 42, paragraphs 1 and 6, of the same TUSMA, it is provided that:

[5]When visiting a website that uses age tokens, clicking on a button to verify your age through the provider will prompt you to log in to your age account. You will be asked to enter your username and password. The website checks whether there are age tokens in the user's browser that match the criteria defined by the company linked to the user's account. If so, the provider returns a result to confirm that a previous check has already been performed and whether your age token meets the above criteria.

1. *Without prejudice to Articles 14 to 17 of Legislative Decree No. 70 of April 9, 2003, providers of video-sharing platforms subject to Italian jurisdiction must take appropriate measures to protect:*
   a) minors from programs, user-generated videos, and audiovisual commercial communications that may harm their physical, mental, or moral development in accordance with Article 38, paragraph 3;

   [omissis]

6. *For the purposes of protecting minors referred to in paragraph 1, letter a), the most harmful content is subject to the most stringent access control measures.*

Article 42, on the other hand, regulates the new rules to be applied to providers of video-sharing platform services established or considered to be established in Italy.

With specific reference to age verification tools, paragraph 7 of Article 42 of the TUSMA provides that:

7. *Video sharing platform providers are in any case required to: [omissis]*

   f) set up systems to verify, in compliance with personal data protection legislation, the age of users of video sharing platforms with regard to content that may be harmful to the physical, mental, or moral development of minors;

   [omissis]

   h) equip themselves with parental control systems under the supervision of the end user with regard to content that may be harmful to the physical, mental, or moral development of minors;

Finally, Decree-Law No. 123 of September 15, 2023, converted with amendments by Law No. 159 of November 13, 2023, introduced *"Urgent measures to combat youth hardship, educational poverty, and juvenile crime, as well as for the safety of minors in the digital environment"* (hereinafter referred to as *the Decree*).

In particular, Article 13-bis, entitled *'Provision for verifying the age of majority for access to pornographic sites'*, establishes that:

1. *Minors are prohibited from accessing pornographic content, as it undermines respect for their dignity and compromises their physical and mental well-being, constituting a public health problem.*
2. *Without prejudice to the provisions of Article 42 of Legislative Decree No. 208 of November 8, 2021, website operators and video sharing platform providers that distribute pornographic images and videos in Italy are required to verify that users are of legal age in order to prevent minors under the age of 18 from accessing pornographic content.*
3. *Within sixty days of the date of entry into force of the law converting this decree, the Communications Regulatory Authority shall establish, by its own provision, after consulting the Data Protection Authority,* ***the technical and procedural methods*** *that the subjects referred to in paragraph 2 are required to adopt to verify the age of users, ensuring an adequate level of security*

to the risk and compliance with the minimization of personal data collected for the purpose.

4. *Within six months of the date of publication of the provision referred to in paragraph 3, the subjects referred to in paragraph 2 shall equip themselves with effective systems for verifying the age of majority in accordance with the requirements set out in the aforementioned provision.*
5. *The Communications Regulatory Authority shall monitor the correct application of this article and, in the event of non-compliance, shall notify the parties referred to in paragraph 2, even ex officio, of the violation, applying the provisions of Article 1, paragraph 31, of Legislative Decree No. 249 of July 31, 1997, and shall warn them to comply within twenty days. In the event of failure to comply with the warning, the Communications Regulatory Authority shall take all necessary measures to block the site or platform until the parties referred to in paragraph 2 restore conditions of supply that comply with the contents of the Authority's warning.*

This provision therefore provided for the introduction of new tools to protect minors from pornographic content, images, and videos disseminated in Italy by "*website operators" and "video sharing platform providers."*

In light of the regulatory framework outlined above, and with a view to making it effective, the Authority, within the scope of its institutional duties, has initiated, by Resolution No. 9/24/CONS, a procedure involving all parties concerned in various capacities, with a view to adopting a measure establishing the technical and procedural methods that the parties referred to in paragraph 2 of Article 13-bis of *the Decree* are required to adopt to verify the age of users, ensuring a level of security appropriate to the risk and compliance with the minimization of personal data collected for the purpose.

Article 3 of the aforementioned resolution provided for the launch of a 30-day public consultation through the publication of a resolution by the Authority with an attached consultation document.

In accordance with the provisions of Article 3 of the resolution, the Authority, following the consultation, obtained the opinion of the Data Protection Authority.

This approach was considered the most effective given the variety of possible solutions for verifying the age of users, which could potentially create different levels of protection for minors and, at the same time, protection of personal data.

III. Measures at European level

At European level, there have been various regulatory provisions aimed at protecting minors from content disseminated on online digital platforms that could harm their moral, physical, and psychological development.

In particular, Directive (EU) 2018/1808 of November 14, 2018, which amended Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation, or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive), added, in Article 1 of Directive 2010/13/EU, letter a-bis) introducing the definition of "*video-sharing platform service*" as *"a service as defined in Articles 56 and 57 of the Treaty on the Functioning of the European Union, where the main purpose of the service, a distinguishable section thereof, or a feature thereof*

essential is the provision of programs, user-generated videos, or both, to the general public, for which the video-sharing platform provider has no editorial responsibility, for the purpose of informing, entertaining, or educating via electronic communications networks within the meaning of Article 2(a) of Directive 2002/21/EC, and whose organization is determined by the video-sharing platform provider, including by means of automatic means or algorithms, in particular through display, letter a) of Directive 2002/21/EC and whose organization is determined by the video-sharing platform provider, including by automated means or algorithms, in particular through display, tagging, and sequencing."

Furthermore, the aforementioned Directive noted in Recital (45) that *"New challenges arise, in particular in relation to video-sharing platforms, where users, in particular minors, increasingly consume audiovisual content. In this context, harmful content and hate speech made available on video-sharing platform services are a growing concern. In order to protect minors and the general public from such content, it is necessary to establish proportionate rules on these issues."*

Furthermore, the aforementioned Directive also noted in Recital 47 that "*A significant proportion of the content made available on video-sharing platform services is not under the editorial responsibility of the video-sharing platform provider. However, those providers generally determine the organization of the content, i.e., programs, user-generated videos, and audiovisual commercial communications, including in an automated manner or by means of algorithms. They should therefore be required to take appropriate measures to protect minors from content that may impair their physical, mental, or moral development. They should also be required to take appropriate measures to protect the general public from content that incites violence or hatred against a group or a member of a group on any of the grounds referred to in Article 21 of the Charter of Fundamental Rights of the European Union (the Charter) or whose dissemination constitutes an offense under Union law.*

The aforementioned Directive introduced Article *28-ter* of Directive 2010/13/EU, pursuant to which paragraph 1 provides that *"Without prejudice to Articles 12 to 15 of Directive 2000/31/EC, Member States shall ensure that video-sharing platform providers under their jurisdiction take appropriate measures to protect: (a) minors from programs, user-generated videos, and audiovisual commercial communications that may impair their physical, mental, or moral development in accordance with Article 6a(1).*

Finally, Article *28-ter*(3) provides that Member States shall ensure that all providers of video-sharing platforms under their jurisdiction apply appropriate measures to protect their users, determined in light of the nature of the content in question and the harm it may cause, and that are practicable and proportionate; in particular for the protection of minors, it provided that the most harmful content disseminated on a video-sharing platform should be subject to the most stringent access control measures. To this end, it has provided in letter f) that these measures consist, as appropriate, of activities to "*establish and apply systems to verify the age of users of video-sharing platforms with regard to content that may harm the physical, mental, or moral development of minors."*

The recent Regulation (EU) 2022/2065 of October 19, 2022, on a single market for digital services and amending Directive 2000/31/EC (Digital Services Act or DSA) defined, in Article 1, paragraph 1, letter i), *online* platforms as: "*an information storage service which, at the request of a recipient of the service, stores and disseminates information to the public, except where such activity is a minor and purely ancillary function of another service or minor functionality of the main service and, for objective and technical reasons, cannot be used without that other service and provided that the integration of that function or functionality into the other service is not a means of circumventing the applicability of this Regulation*";

With this regulation, the European Commission has taken action on this issue, supporting and promoting the implementation of rules aimed at protecting minors online: in particular, Article 28 of *the Digital Services Act* requires all providers of online platforms accessible to minors to take appropriate and proportionate measures to ensure a high level of privacy, security, and protection of minors, primarily through the activation of age verification mechanisms as explained below.

In particular, Article 35 of the aforementioned Regulation stipulates that providers of very large *online* platforms and very large online search engines must take reasonable, proportionate, and effective mitigation measures tailored to the specific systemic risks identified in accordance with Article 34, paying particular attention to the effects of such measures on fundamental rights. In particular, paragraph 1(j) provides that such measures may include, where appropriate: *"the adoption of targeted measures to protect the rights of minors, including age verification and parental control tools, or tools to help minors report abuse or obtain support, as appropriate*."

The adoption of the eIDAS Regulation[6]in 2014 enabled Member States to use national electronic identification (eID) schemes to access cross-border *online* public services. As the digital landscape has evolved, both in terms of public and private sector services offered *online*, there has been a growing need to identify and authenticate users with a high level of assurance. At the same time, threats to digital privacy have become apparent and the risks of profiling and surveillance of individuals have increased. Therefore, in 2021, the European Commission proposed a revision of the original 2014 regulation, based on the principle that all citizens should have the ability to control their digital identity through the creation of an ***EU digital identity wallet (***hereinafter referred to as the EUDI wallet). Citizens should be able to carry their digital identity with them throughout the EU, moving seamlessly across borders without ever losing control of their data, with privacy and security at the heart of the project. The wallet supports the principles outlined in the EU Declaration on Digital Rights and Principles([7]) and contributes to achieving the Digital Decade Policy Agenda([8]) goal of ensuring that 100% of EU citizens have access to digital identity by 2030.

In **April 2024**,the European Council definitively approved the proposed amendment to the regulation concerning the establishment of a new framework for a European digital identity[9]. The aim is to have a digital identity system that is recognized throughout Europe, regardless of the state in which this system is made available (harmonized digital identity framework).

The Regulation **requires Member States to issue a European digital identity wallet**[10] as part of an electronic identification scheme **in line with common technical standards**, following a mandatory conformity assessment and voluntary certification in the

[6]Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS)

[7]https://digital-strategy.ec.europa.eu/en/policies/digital-principles

[8]https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en

Regulation 2024/1183 of the European Parliament and of the Council of April 11, 2024, amending Regulation (EU) No 910/2014 as regards the establishment of the European Digital Identity Framework.

(10) TheEuropean Digital Identity Wallet is defined as a product or service that enables the user to store identity data, credentials, and attributes linked to their identity, provide them on demand to relying parties, and use them for authentication, online and offline, for a service, in accordance with Article 6a of the eIDAS Regulation, as well as to create qualified electronic signatures and qualified electronic seals.

context of the European cybersecurity certification framework, as established by the Cybersecurity Regulation[11] . The provisions are designed to ensure that natural and legal persons have the possibility to request and obtain, store, combine, and use personal identification data, electronic attributes, and electronic attribute certificates for *online and offline* authentication and for accessing public and private goods and services *online,* with full user control.

One of the reasons behind the Regulation is that, in most cases, citizens are currently unable to exchange information relating to their identity, such as addresses, age, professional qualifications, driving licenses, other permits, and payment details, digitally across borders in a secure manner and with a high level of data protection. Therefore, the EUDI wallet would overcome these limitations by offering the possibility to exchange the minimum identity attributes necessary to access certain *online* services that require authentication, such as proof of age. In addition, the new eIDAS Regulation provides that, **where very large online platforms, as defined by the DSA, require users to authenticate themselves in order to access online services, they must also accept the use of European digital identity wallets, strictly on a voluntary basis, including for the minimum attributes necessary for the specific *online* service for which authentication is required, such as proof of age[12] .**

In addition, it is envisaged that EUDI wallet users will also have access to a free qualified digital signature feature.

By 2026, each Member State will have to make a digital identity wallet available to its citizens and accept European digital identity wallets from other Member States.

The Age Verification Task Force

On January 23, 2024, the ***Task Force on age verification*** began its work with the presentation by the Commission of a number of studies carried out by experts in the field.

First, a number of definitions were provided, as outlined below.

Age assurance is the generic term for methods used to determine an individual's age or age range at various levels of confidence or certainty. The three main categories of age assurance methods are **age estimation, age verification, and self-declaration**.

Self-declaration refers to when a user enters a date or selects a box to declare that they are above/below a certain age.

Age estimation consists of methods that establish with a certain probability that a user is of a certain age, falls within an age range, or is above or below a certain age. Age estimation methods include automated analysis of behavioral and environmental data, comparing how a user interacts with a device with other users of the same age, and metrics derived from movement analysis or testing their abilities or knowledge.

[11] Consists of a set of technologies, processes, and protective measures designed to reduce the risk of cyberattacks
[12] Paragraph 3 of Article 12-ter introduced by the eIDAS 2.0 Regulation

Age verification is a system based on rigid (physical) identifiers and/or verified sources of identification that provide a high degree of certainty in determining a user's age. It can establish a user's identity but can also be used to establish minimum age.

Among the various actions related to the subject of this consultation, the Commission intends to create a European standard on online age verification by defining requirements for age verification solutions for industry.

In this context, the *Age Verification Task Force* will discuss and support the development of a European framework and approach to age verification, as well as ensuring consistency and a common approach across the EU.

A study presented by experts commissioned by the Commission summarizes the age verification methodologies identified:

- **Self-declaration:** users declare their age/age group without providing further evidence.
- **Hard identifiers:** users provide verified identity documents (e.g., passport) to prove their age.
- **Credit cards:** use of credit card data to verify that a user is over 18 years of age.
- **Blockchain-based identity:** use of decentralized technologies such as blockchain to create digital identities for users, in order to use these identities for age verification.
- **Account holder confirmation:** relying on confirmation from an existing verified account holder that another user is of the required age to use the platform.
- **Multi-platform authentication:** Use existing user accounts with large platforms (e.g., Google, Apple, etc.) to authenticate a user's age for other products/services.
- **Facial estimation:** using artificial intelligence to analyze a person's facial features to estimate their age.
- **Behavioral profiling:** using artificial intelligence to analyze users' online activity to estimate their age.
- **Aptitude testing:** testing the user's ability or aptitude to estimate their age.
- **Third-party age assurance services:** using third-party companies for age assurance services. Third parties may use any of the other methods for age assurance.

The following requirements were identified in the study:

i. **Proportionality and subsidiarity:**

- A general requirement that may play a role in meeting other requirements.
- Balance between the means used to achieve the set objective and its impact on the restriction of people's rights.
- Use of the least invasive means to achieve the set objective.

ii. **Privacy:**

- The data protection principles established by the GDPR (data minimization, accuracy, storage limitation, etc.) must be followed.
- High level of privacy protection for minors (OSA).

- Age verification may conflict with privacy rights.

iii. **Security:**

- Sufficient cybersecurity measures must be implemented (GDPR, CRA proposal).
- The sophistication of cyberattacks makes achieving cybersecurity difficult but also more important.

iii. **Accuracy and effectiveness:**

- Accuracy is important to ensure the safety of children online.
- However, accuracy may have an inverse relationship with privacy.
- Full accuracy is difficult to achieve but should be pursued.

iii. **v. Functionality and ease of use:**

- Age assurance technologies should be easy to use and based on children's evolving abilities.
- Functionality can encourage user adoption.
- However, functionality may dilute effectiveness.

vi. **Inclusivity and non-discrimination:**

- Non-discrimination is one of the four general principles of the UN CRC.
- Differences among children in terms of language, ability, socioeconomic status, etc. should be taken into account when age assurance is implemented.
- Age verification could lead to discrimination and exclusion in various ways.

vi. **Promoting participation and access:**

- Age verification should not equate to mistakenly blocking children or providing them with inferior services.
- Digital technologies empower children, and age verification should not hinder this, but rather encourage it.

viii. **Transparency and accountability:**

- Age verification providers should be transparent with users about the age verification methods they use, and age verification should be understandable to children.
- Platforms must be responsible for implementing age verification.

viii. **Notification, dispute, and redress mechanisms:**

- Due process should be followed for decisions relating to age assurance.
- There must be channels of communication for notifying, disputing, and seeking redress against incorrect Assurance decisions.

viii. **Listening to the views of minors:**

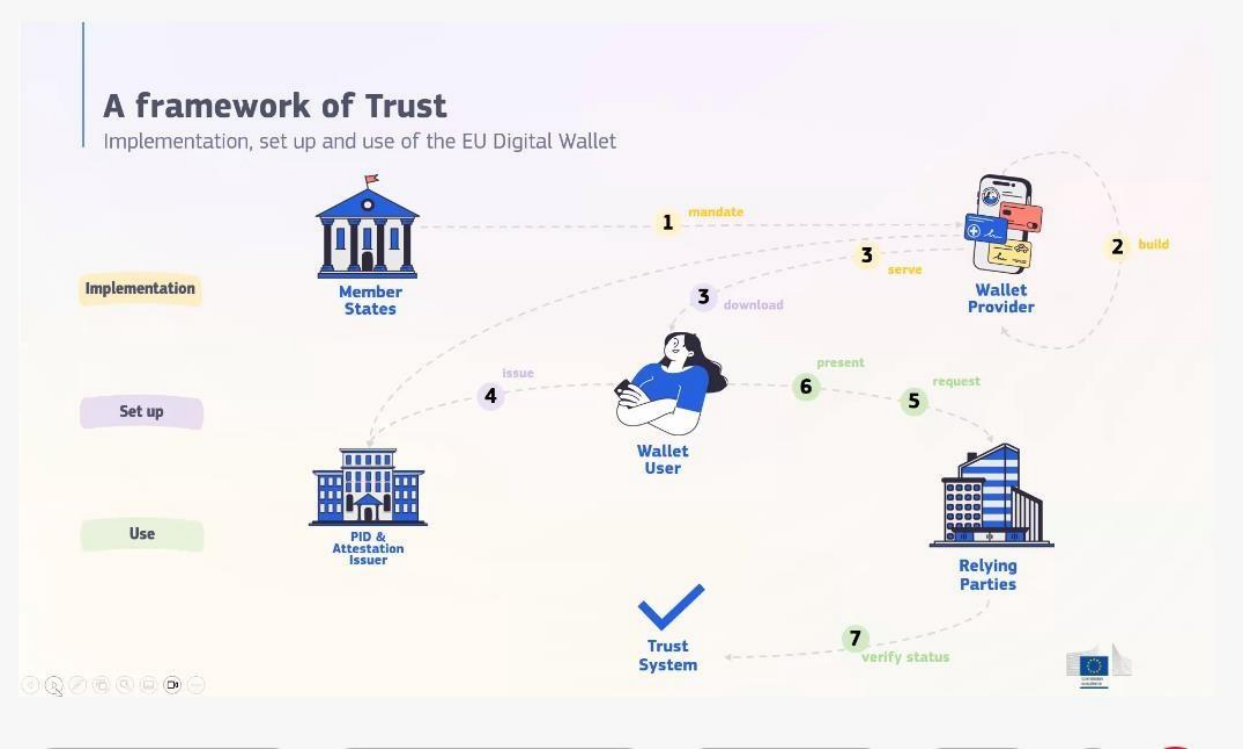
- According to the UN CRC, minors have the right to be heard.

- Platforms should engage with and pay attention to children's views on age verification.

During the meeting on March 18, 2024, representatives of the European Commission presented the EUDI wallet implementation project[13],which aims to define a *framework* of rules and specifications common to all member states for the creation of digital identity management wallets. European citizens, residents, and businesses will be able to use the wallet app to securely obtain, store, and share important digital documents and will be able to easily prove who they are when accessing *online* digital services.

The basic assumptions underlying the project are to **keep the user's identity hidden when proof of age is requested, and that any third parties involved in the age verification process are not aware of the user's intended use of the certification**.

The process envisaged by the Commission for the implementation, set-up, and use of the EUDI wallet follows the outline below.



Initially, Member States mandate (steps 1 and 2) providers (*wallet providers*) to implement digital identity wallets in accordance with *the framework* defined by the Regulation, developing, for example, a wallet app that users can download to their mobile devices.

Using the digital identity wallet app, users can store and manage their digital identity, as well as any attributes (e.g., age, nationality, gender, etc.) and certificates (e.g., proof of age, driver's license, educational certificates, etc.) validated by specific issuers (*PID & Attestation*

[13] https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/

issuer, steps 3 and 4) that interact with *digital wallet* providers. Users will then be able to use their digital identity wallet to identify and authenticate themselves *online* when requested by public/private entities to access their services (*relying parties*, steps 6 and 5).

With regard to age verification using the digital identity wallet, the Commission has outlined **the key requirements underlying the project**:

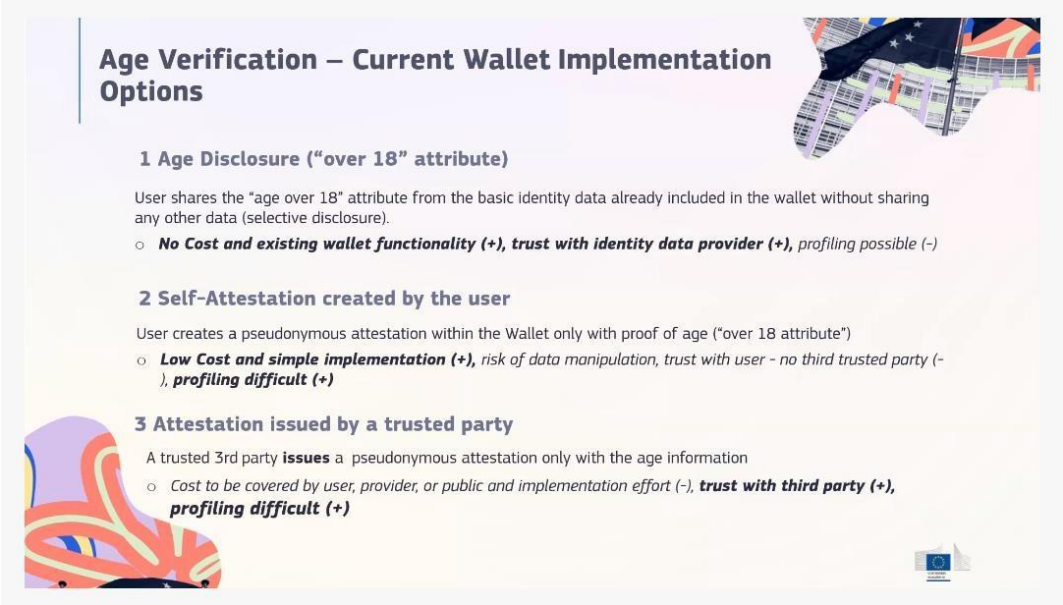
- Provide proof of age (+18) *online* when requested by a service provider/platform;
- **The proof of age must not disclose any personal information about the user**;
- **The proof of age must not disclose any information about the age verification process to any of the third parties involved in the process**;

With regard to age verification mechanisms, the Commission has proposed four scenarios for processes that will be made available to users using the EUDI wallet. **The assumptions are that the user's identity will remain hidden when proof of age is requested, and that any third parties involved in the age verification process will not be aware of the user's intended use of the certification**.

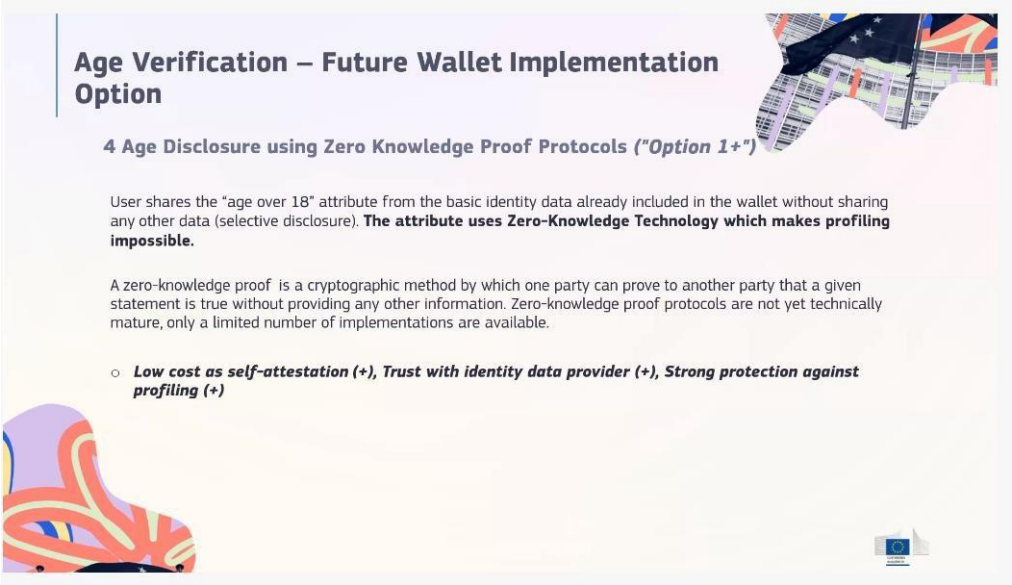
The first scenario (*Age Disclosure – over 18 attribute*) consists of the user being able to share the 'adult' attribute based on basic information about their identity, which is stored in *the digital wallet*, without providing any personal data to the provider requesting proof of age.

The second scenario (*self-attestation created by user*) involves the creation of a pseudonymous attestation by the user directly within the *digital wallet*, which includes only the information that the user is of legal age. This attestation can be sent to the provider requesting proof of age.

The third scenario (*attestation issued by a trusted third party*) involves the generation of a pseudonymous attestation by a certified third party, which contains only the information that the user is of legal age.



A fourth scenario (*Age disclosure using zero knowledge proof protocols*), which is expected to be implemented in the future, involves the use of "zero-knowledge" **encryption protocols** with which the user can generate attestations of age without sharing any other personal information and avoiding profiling by providers requesting proof of age and other third parties involved in the process.

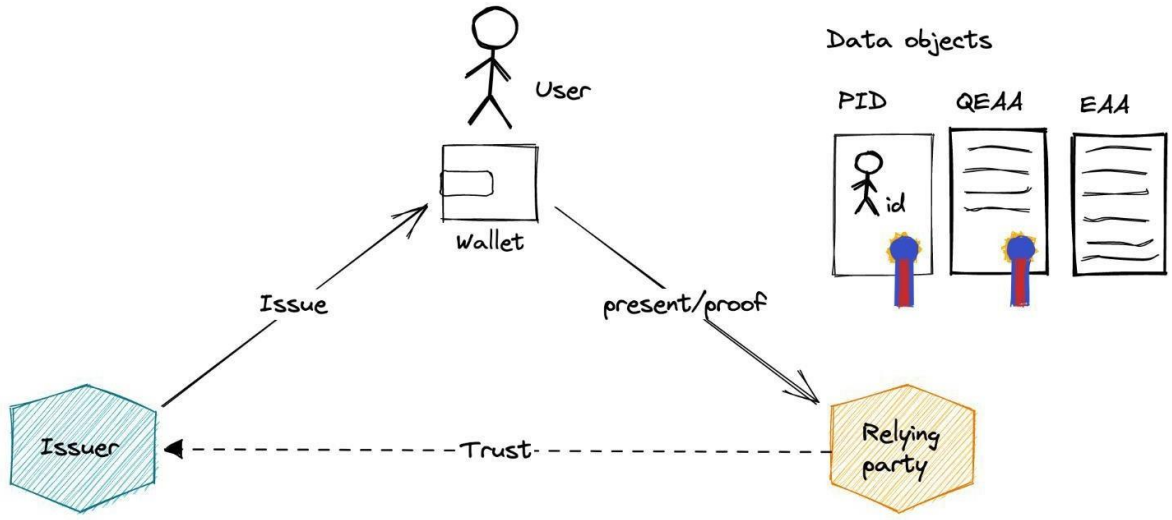


The Commission has developed a pilot version of *the digital wallet*, which will undergo an initial testing phase involving volunteer member states. During this phase (known as *POC - Proof of Concept)*, any comments and suggestions from member states on the mechanisms for verifying age implemented through the *wallet* will be taken into account.

The Commission will then proceed, in the second half of 2024, to launch the large-scale pilot project at European level with the aim of **making the digital identity wallet available to users from 2026**.

As part of the work carried out on April 23, 2024, aimed at launching PoC activities with the active participation of Member States, the Commission provided further details on the mechanisms that will be implemented for age verification through the European Digital Identity Wallet.

The following diagram shows the different entities involved in the request, certification, and verification process, namely the *user* who uses the digital wallet, *the issuer* who provides proof of age, and the *relying party* to whom the user presents proof of age.



As shown in the figure, the objects managed by the digital identity wallet are *Personal Identification (PID), Electronic Attestation of Attributes (EAA), and Qualified Electronic Attestation of Attributes (QEAA):*

1. **PID (Personal Identification):** this is a set of data that is issued in accordance with EU regulations or national laws and allows the identity of a natural person to be established. The PID includes both mandatory information (name, nickname, date of birth) and optional information (age in years, surname at birth, residential address, country of residence, nationality);
2. **EAA (electronic attestation of attributes):** consists of an electronic certificate that allows the authentication of specific attributes [14] (e.g., "legal age");
3. **QEAA (qualified electronic attestation of attributes):** an electronic certificate issued by a (qualified) trust service provider, such as a driver's license, proof of legal age, etc.

As established by the Commission, the PoC activities will focus on the following two scenarios:

- **Scenario 1 - disclosure of age (attribute "being 18 years old")**

The user shares the attribute "age over 18" from the basic identity data already included in the wallet without sharing any other data (selective disclosure). In this case, the site/platform asks the user to verify their age by providing them with a QR code. The user, by scanning the QR code using the digital wallet app, receives a request to present the information contained in the PID (e.g., "legal age" attribute) and allows the requested information to be shared. The website/platform thus receives the legal age information from the digital wallet.

- **Scenario 2 - certification (pseudonym) issued by a trusted party**

[14] An 'attribute' is defined as a prerogative, characteristic, or quality of a natural or legal person or entity, in electronic form.

A trusted third party issues a pseudonymous certificate[15]containing only age information. In this case, the user asks a certification authority to issue a certified certificate of age. The certification authority asks the user to share their PID information in order to issue a pseudonymous certificate of age. The website/platform asks the user to verify their age by providing a QR code. The user, by scanning the QR code using the digital wallet app, receives a request to present the pseudonymous certificate of age and allows the required information to be shared. The website/platform thus receives the age information from the digital wallet.

Working Group No. 6 "Protection of Minors"

In July 2024, the DSA board defined the structure of the technical working groups tasked with developing the various activities planned by the DSA during 2025. Among these, working group no. 6, *"Protection of* Minors" (hereinafter WP6), was established, in which the Authority actively participates with its designated experts.

WP6 is responsible, among other things, for defining the technical specifications of the *age verification* solution to be implemented by the supplier selected by the European Commission as part of the tender launched on October 15, 2024, for the development of a European age verification solution[16]. The project involves the creation of a 'white label APP([17]) ' based on the specifications established by the group, which will be made available to Member States during the first quarter of 2025, in order to ensure the availability of a European solution pending the completion of the development of the European digital identity wallet (EUDI Wallet) scheduled for the end of 2026.

In addition, WP6 is responsible for defining guidelines relating to Article 28 of the DSA in order to assist providers of online platforms accessible to minors in applying appropriate and proportionate measures to ensure a high level of privacy, security, and protection of minors on their service.

IV. Standardization and regulatory initiatives

At European level and, more generally, at international level, numerous initiatives have been implemented or are currently being developed. An overview of these initiatives is provided **in Annex 1** to this document, to which reference should be made.

[15] The term "pseudonym" refers to an identifier that uniquely represents a user and does not contain any reference, data, or information about the user's attributes or personal data.

[16] The European Commission selected Deutsche Telekom AG and Scytáles AB as suppliers following the conclusion of the tender procedure published on following link https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/tender-details/ae950883-112f-4139-989e-1c8d794bb77a-CN

[17] White label software is generic software designed to be customized, configured, and distributed by other distributors, allowing them to superimpose their own brand, identity, or other characteristics.

ANNEX 1

I. Standardization and regulatory initiatives

Numerous initiatives have been implemented or are underway at European or, more generally, international level. An overview of these initiatives is provided in Annex 1 to this document, to which reference should be made.

I.1 The euConsent project

This is a European project, co-funded by the EU, which aims to develop an interoperable, browser-based *age assurance* method.

As part of the euCONSENT project, a document, still in draft form, entitled "ISO Working Draft Age Assurance Systems Standard" has been published.

Below are some elements of the document that are considered useful for the preparation of technical specifications on age verification processes.

Characterization of age verification systems

In the aforementioned document, the term *"age assurance*" refers to a process of determining and communicating an individual's age. Age verification can be conducted through one or more *identity attribute* verification processes that do not necessarily require full identity verification and can operate on a federated model.

Age assurance can apply to specific ages or age ranges (age classification). According to the document, **an age assurance system** consists of:

(a) One or more **verification components** that indicate a person's age,

(b) A **processing subsystem** that analyzes the *level of confidence* that can be applied to age *verification components* (the degree to which an *age attribute* can be considered reliable; reliability is classified below as "zero," "basic," "standard," "enhanced," or "rigorous" in accordance with certain ISO standards), and communicates this to a party that relies on such verification (in cases where the site provider is different from the entity performing the age verification). *Age attribute* means the characteristic or property of an entity, in this case age (e.g., over 18 years of age). *Attribute* means the characteristic or property of an entity, in this case age (e.g., over 18 years of age).

The ***components of verifying*** an individual's age may include:

(a) A process or system that obtains an *age attribute* from a document (e.g., passport),

(b) A process or system that derives an *age attribute* from other *primary or secondary credentials* (see explanation below),

(c) A process or system that uses *artificial intelligence* (a branch of computer science dedicated to the development of data processing systems that perform functions normally associated with human intelligence, such as reasoning, learning, and self-improvement) to ascertain age from one or more biometric identifiers, behaviors, characteristics, or actions of individuals.

(d) A process or system that implements social *proofing* (analysis, with the user's consent, of their digital footprint and related social graphs, which can be queried to assess the veracity of a self-asserted age guarantee) to obtain or verify age attributes.

social graphs—which can be queried to assess the veracity of a self-asserted age guarantee) to obtain or verify age attributes.

(e) A process or system based on the attestation of trusted parties (such as parents or legal guardians).

(f) An assessment, in person or online, conducted by a qualified person who evaluates elements that take into account a person's appearance, behavior, background, and credibility.

(g) A process or system that derives age attributes from any other method capable of establishing *confidence levels* as described in this document.

An age assurance ***processing subsystem*** may include:

(a) A process or system for bringing together *verification components* from multiple sources,

(b) A process or system for identifying potential attacks by malicious actors, protecting against *presentation attacks*, and assessing the "liveness" of individuals.

(c) A process or system for identifying and addressing *counter-indicators* (evidence or information that casts doubt on or otherwise indicates that the stated age may not be the actual age).

(d) A process or system for increasing trust (the degree to which an entity has confidence in the accuracy and reliability of age verification processes) in an *age attribute* across multiple sources,

(e) Ability for individuals to exercise their data rights,

(f) A process or system for transmitting age attributes, at a declared level of age assurance, to relying parties,

(g) A process or system for monitoring, continuously improving, and learning from age verification activities.

Primary and secondary credentials

Age verification systems should pay particular attention to the difference between primary and secondary credentials.

A **primary credential** is a tool, document, or record issued by an authoritative entity and used by an individual to provide proof of age. The authoritative entity may be a public body or a private entity established for this purpose. The inherent risk that the primary credential may have been issued inappropriately, to the wrong person, with incorrect data, or may have been falsified should be considered.

A **secondary credential** is an attribute relating to an individual derived from a primary credential. For example, the creation of a record in the banking system of data relating to a natural person constitutes the creation of a secondary credential. The bank opens the account after acquiring data from an individual's passport. The bank's examination of that passport is the examination of a primary credential.

Age verification systems can rely on both primary and secondary credentials, but must take additional risk-assessed approaches to managing secondary credentials, including the potential for errors in data capture and constraints, regulatory oversight, and the reliability of the secondary credential producer.

Countermeasures

Age verification systems may implement multiple verification components and may have multiple sources of information from both primary and secondary credentials. This could lead to incorrect data matches or information indicating that the declared age may not match the actual age. These are called counterindicators.

Age assurance system providers have two options when presented with a counterindicator:

(a) Take action to resolve the counter-indicator by gathering additional evidence to support the declared age; OR

(b) Communicate the existence of the counter-indicator to each relying party.

Classification of age assurance levels

The level of confidence associated with an age attribute can be determined by the process used to acquire, validate, and verify the declared age in the age verification system. The level of confidence can be established by the regulator based on the protected asset, in this case, the health of the minor. Below are the five *levels of confidence* described in the aforementioned document.

1. Zero Level of Assurance of Age Verification

This level corresponds to processes based on the age declared by the individual through self-declaration and without the application of age verification components. No attempt is made to validate the claimed age attribute.

Changes in the declared age over time represent a so-called counter-indicator.

2. Basic level of assurance of age verification

In addition to the age declared by the individual, at least one age verification component tested at assurance level 1 (EAL1) is applied (the draft document provides for seven assurance levels, from EAL1 to EAL7, corresponding to increasing levels of effort for verification and testing of the design).

The system acquires the age declaration by referring to questions asked to the individual, inviting the user to submit evidence to support a component of the age assurance process.

The age assurance process component may include simple validation of the declared age attribute. The process must not result **in a false acceptance or false rejection** rate **greater than 5%.**

The baseline level includes systems to reduce attempts at circumvention (attack vectors) by bots or automated processes or by false or inaccurate self-declarations, as well as techniques to establish an individual's liveness. Such attempts should be supported by methods to reduce or eliminate systemic bias in the age verification process. A basic age guarantee may leave unresolved counter-indicators, which should be communicated to the party relying on the verification.

Authentication must be renewed at least every 3 months.

3. Standard Assurance Level for age verification

In addition to acquiring the age declared by the individual, at least one age assurance component tested at assurance level 2 (EAL2) is applied.

The system acquires the age declaration by referring to questions asked to the individual, inviting the user to submit evidence to support a component of the age assurance process.

The age assurance component process must include validation of the declared age attribute. The process must not result in a false acceptance or false rejection rate greater than 1%.

If the process is undertaken remotely, it shall be necessary to establish the liveness of the individual in accordance with ISO/IEC 30107. The failure rate shall be less than 1%.

If the process involves the use of artificial intelligence, the classification error or statistical parity error due to the unique characteristics of individuals must not exceed a variance of 3%.

The process includes mechanisms to discourage the submission of false or inaccurate self-declarations. The system must prevent attacks by bots or automated processes and recognize false or inaccurate self-declarations. This includes verifying the liveness of an individual. Such countermeasures must be based on methods that reduce or eliminate systemic biases in the age verification process.

All identified countermeasures must be resolved or communicated to the relying party.

Authentication should be renewed at least every month.

4. Enhanced Assurance Level of Age Verification

In this case, at least two additional age assurance components from two independent sources (one of which must be a primary or secondary credential) must be added to the declared age (implicit or actual self-declaration).

The age assurance components must be tested up to assurance level 3 (EAL3).

Processes related to the age assurance component must include validation of the declared age attribute. The process must not result in a false acceptance or false rejection rate greater than 0.1%.

If the age verification process takes place online, it shall be necessary to establish the vitality of the individual in accordance with ISO/IEC 30107. The failure rate shall be less than 1%. If the process involves the use of artificial intelligence, the classification or result error rate for protected characteristics of individuals shall not exceed a variance of 3%.

The process includes mechanisms to discourage the submission of false or inaccurate self-declarations. All identified counter-indicators must be resolved or communicated to the relying party. Authentication should be renewed at least weekly.

5. Strict Level of Assurance of Age Verification

Implicit or actual self-declaration is supplemented by verification of at least two other age assurance components from two independent sources (one of which must be a primary credential) to validate the declared age.

Age assurance components must be tested up to assurance level 4 (EAL4). The age assertion can be acquired in a data acquisition process by inviting the user to submit evidence to support the age assurance component processes.

The processes related to the age assurance component must include validation of the declared age attribute. The process must not result in a false acceptance or false rejection rate greater than 0.01%. If the process is undertaken remotely, it shall be necessary to establish the vitality of the individual in accordance with ISO/IEC 30107. The failure rate shall be less than 1%.

If the process involves the use of artificial intelligence, the classification or result error parity for the protected characteristics of individuals must not exceed a variance of 3%. The process includes mechanisms to discourage the submission of false or inaccurate self-declarations. All identified counter-indicators must be resolved or communicated to the relying party. Age verification should be repeated for each age-related eligibility decision, repeating the age assurance process.

The issue of security: cyber attacks, attempts to circumvent the verification process, and counter-indicators

All processes are more or less vulnerable to cyber attacks or attempts by minors themselves to circumvent the verification system. Age verification systems should identify possible vulnerabilities in the process, such as:

(a) Accuracy, reliability, and risk of fraud of the data source, including consideration of the risks associated with inferring or deriving data from other sources used for other purposes;

(b) The possibility of an attack on the system;

(c) The possibility for an individual to circumvent the system;

(d) The possibility of collusion or complicity between parties (including between minors and adults);

For online age verification, system developers should assess the risk that a non-human process could be used for a system-level attack. Therefore, a system for detecting so-called liveness, as defined by ISO/IEC 30107, becomes important.

Other types of attacks, known *as presentation attacks*, may occur:

(a) by acquiring biometric data directly from a person, online or via existing databases, and using it for biometric spoofing (e.g., a picture of a person's face or video on a tablet, or a fake silicone or gelatin fingerprint) to a biometric sensor;

face or video of a person on a tablet or a fake silicone or gelatin fingerprint) to a biometric sensor;

(b) Another example of a presentation attack can be found in relation to a forged document (e.g., a fake driver's license, a forged passport, or a forged registration in a database).

The reliability of the age verification system must be assessed with regard to this type of attack.

I.2 The public consultation by the UK regulator OFCOM

On December 5, 2023, Ofcom launched a public consultation on a guidance document on "highly effective" age checks to be implemented by online service providers to prevent minors from accessing online pornographic services.

The age verification methods considered by OFCOM include checking photo ID, estimating age through facial recognition, and using credit cards.

Service providers are required to safeguard user privacy and the right of adults to access legal pornography.

The published document reports that the latest research shows that the average age at which minors first access online pornography is 13, although almost a quarter do so at the age of 11 (27%) and one in ten at the age of 9 (10%). In addition, almost 8 in 10 young people (79%) had accessed violent pornography depicting coercive, degrading, or painful sexual acts before the age of 18.

The Online Safety Act requires websites and apps that display or publish pornographic content to ensure that minors are not normally able to access pornographic material on their services.

To this end, they are required to introduce an 'age assurance' system – through age verification, age estimation, or a combination of both – that is 'highly effective' in correctly determining whether a user is a child or not**.**

Highly effective methods for age assurance

Under the aforementioned law, OFCOM has been tasked with adopting guidelines to support online pornography service providers in fulfilling their legal responsibilities and to oversee implementation. The draft guidelines set out criteria that age verification checks must meet in order to be considered highly effective; the criteria are based on the principles of technical accuracy, robustness, reliability, and fairness.

The right to privacy and, for adults, to access legal pornography remains unaffected.

Given that the technology underlying age verification is likely to develop and improve in the future, the guidelines include a non-exhaustive list of methods that OFCOM currently considers to be highly effective. These include:

- **Banking**. A user can consent to sharing banking information confirming they are over 18 with the online pornography service. Their full date of birth is not shared.

- **Photo ID matching**. Users can upload a photo ID, such as a driver's license or passport, which is then compared to an image of the user at the time of upload to verify that they are the same person.
- **Facial age estimation**. A user's facial features are analyzed to estimate their age.
- **Mobile network operator age verification**. Some mobile operators in the United Kingdom automatically apply a restriction that prevents children from accessing age-restricted websites. Users can remove this restriction by proving to their mobile operator that they are over 18, and this confirmation will then be shared with the online pornography service.
- **Credit card checks**. In the UK, credit card issuers are required to verify that applicants are over 18 before providing them with a credit card. A user can provide their credit card details to the online pornography service, after which a payment processor sends a request to verify the card's validity to the issuing bank. Approval by the bank can be considered proof that the user is over 18.
- **Digital identity wallets**. Using a variety of methods, including those listed above, users can securely store their age in a digital format, which the user can then share with the online pornography service.

In its guidelines, OFCOM provides examples of age verification approaches that do not meet the standards set out in the draft guidelines. Unreliable methods include:

- self-declaration of age;
- online payment methods that do not require a person to be 18 years old (debit cards, Solo, or Electron); and
- general terms, disclaimers, or warnings.

Services should not host or allow content that directs or encourages minors to attempt to circumvent age and access controls.

I. Introduction to the Guidelines on age verification obligations.

The OFCOM Guidelines on age verification obligations are designed to ensure that regulated service providers take appropriate measures on their systems to ensure that minors are not normally able to access pornographic content by implementing an age verification process (the term age verification is to be understood in a general sense and depends on the methodology used. In some cases, age verification is carried out by means of an estimate of age. In other cases, it is carried out by means of indirect verification of credentials provided by other entities, etc.).

In general, the Guidelines provide guidance on:

- types of age verification systems that can be considered effective and those that are not;
- criteria that service providers should consider when designing or implementing an age verification system to ensure that it is effective;
- principles that service providers should consider to ensure that the age verification process is user-friendly and does not unduly prevent adults from accessing legal content;
- examples where a service provider is likely to be considered to have failed to comply with its age verification obligations.

In the following, the following definitions shall apply:

• **age verification method means** the particular system or technology that underpins an age verification process; and

• **age verification process means** the end-to-end process through which an age verification method or combination of methods is implemented to determine whether a user is a minor.

General guidance on the types of age verification systems that can be considered effective

Age verification obligations require service providers to ensure that minors are not normally able to access pornographic content by implementing an age verification process that is effective in correctly determining whether or not a user is a minor.

This means that providers must implement access controls to their regulated service so that users who have been identified as minors by the age verification process are then prevented from accessing pornographic content (e.g., by denying access to further sections of the service). Service providers must not host or allow content on their services that directs or encourages underage users to circumvent the age verification process or access controls, for example by providing information or links to a virtual private network (VPN).

In general, an age verification process can be considered effective if it is:

• Technically accurate

• Robust

• Reliable

• Fair

Examples of age verification methods that OFCOM considers to be highly effective include:

Open banking Photo ID

matching

Age estimation through facial recognition Age checks by

MNOs

Credit cards

Digital identity wallets

Other methods that meet each of the criteria set out in the Guidelines

Examples of age assurance methods that are not effective Self-declaration

Debit cards, Solo or Electron

Other payment methods that do not require the user to be over 18 General contractual

restrictions on the use of the service by children

Additional features of an age verification process are:

• **Accessibility**

• **Interoperability**

OFCOM acknowledges that there is a wide range of age verification methods that a service provider can implement. Some may be developed internally by the service provider; others may be provided by third-party suppliers. These methods work in different ways, and the technology behind them is likely to continue to improve over time. It should also be noted that new approaches to age verification are likely to emerge in the future.

For this reason, OFCOM has taken an approach to the Guidelines that is not intended to provide an exhaustive list of types of age verification processes that could be effective in correctly determining whether a user is a minor. It does, however, provide examples. This is to ensure, as far as possible, that the Guidelines are future-proof and technology-neutral.

Examples of age verification systems that can be considered effective include established methods such as photo identification matching and more innovative methods such as facial age estimation.

It is up to each service provider to determine which type of age verification method is most appropriate to meet its obligations under the law and these Guidelines.

OFCOM is aware that all age verification methods involve the processing of personal data and, as such, are subject to the relevant legal obligations, to which reference should be made.

Description of criteria for ensuring that the age verification system is effective

In line with the above, OFCOM has deemed it appropriate to provide general criteria for assessing whether a given process can be considered effective in terms of achieving the objective of age verification that is as reliable as possible. The proposed criteria, which must be met simultaneously, are technical accuracy, robustness, reliability, and fairness.

In light of technological developments, OFCOM considers it appropriate to provide guidance on the measurement of each of the above KPIs without defining thresholds at this stage. However, it has asked respondents to provide assessments both in relation to other useful KPIs and in relation to thresholds.

Technical accuracy

The criterion of technical accuracy refers specifically to how well an age verification method can correctly determine a user's age in a test environment (e.g., in a laboratory). The term "technical" accuracy has been used to distinguish this criterion from broader concepts of accuracy, which may take into account a wider range of factors. A typical example is the technical accuracy achievable in the case of age estimation through facial recognition or inference of user behavior. Some studies provide metrics for estimating accuracy. An example is given in the Age Check Certification Scheme (ACCS) document on age assurance measurement technologies, which examined several parameters for evaluating age assurance.

Robustness

The robustness criterion describes the degree to which an age verification method can correctly determine a user's age under unexpected or real-world conditions. To meet this criterion, it appears appropriate for service providers to take the following measures:

a) ensure that age assurance methods have been tested in multiple environments during development;

c) take measures to mitigate circumvention methods that are easily accessible to minors and where it is reasonable to assume that they may use them.

Age verification methods that rely on visual or audio inputs that have only been tested in laboratory conditions may not work effectively in real-world conditions. Different conditions may be due to intentional or unintentional scenarios.

Unintentional scenarios include unexpected variations in input. Examples of circumstances that may affect the effectiveness of an age check in such scenarios include:

a) poor/varying lighting conditions;

b) the use of low-resolution cameras; OR,

c) movement, for example due to a tremor or the natural movement of a hand.

Intentional scenarios include attempts to circumvent the age verification method (it is recognized that any age verification system may be subject to circumvention attempts, even successfully).

Service providers must therefore take measures to ensure that their age verification process can mitigate simple forms of circumvention that are easily accessible to minors and that are permitted by the operation of the age verification method. This refers, for example, to cases where a minor can gain access to pornographic content by using the personal data or forms of identification of an adult or otherwise impersonating them.

Reliability

The reliability criterion describes the degree to which the age result obtained by an age verification method can be considered reproducible and derived from reliable evidence.

For the purposes of a reliable verification system, the service provider is required to:

[18] OFCOM has reported case studies for illustrative purposes in its document.
The first specific example is where the service provider has implemented a method of estimating facial age that requires only a still image. This functionality without additional authentication is at risk of "print attacks," where a printed photograph or image of a user's face is presented to the camera in an attempt to match the image on the photo ID. Liveness detection, which confirms the authenticity of a scanned face by distinguishing it from static images or videos through the analysis of subtle facial movements (e.g., blinking), is one way a service provider can take steps to mitigate this risk.
The second is when the service provider has implemented an age verification process that allows users to verify their age using fake or manipulated identity documents (for example, where the age could be altered using a pen or pencil on an existing ID at one end) or more advanced forms involving the misuse of authentic documents. The former is easily accessible to children and it is reasonable to expect that they could use it. Therefore, where a regulated service uses a method of matching photo ID documents, it is necessary for the service provider to take steps to mitigate the most basic levels of false documentation.
In general, the draft Guidelines recognize that there may be other forms of circumvention of the age verification process or the access control process as a whole. Therefore, service providers need to take measures to mitigate and refrain from promoting such forms. An example of potential non-compliance in this case would be where the service provider explicitly and deliberately encourages underage users to circumvent the age verification process and/or access controls for UK users, for example by providing a link and recommending the use of a VPN to enable them to access pornographic content from regulated providers.

a) ensure that age verification methods with a degree of variance (e.g., methods based on statistical models or artificial intelligence) have been adequately tested and that performance is measured and monitored; AND,

b) Ensure that the evidence used by the age verification method comes from a reliable source.

Fairness

The fairness criterion describes the extent to which an age verification method avoids or minimizes errors and discriminatory results, such as lower technical accuracy for users of certain ethnicities when based on facial recognition. Relevant characteristics for this indicator include race, age, disability, sex, and gender.

In order to ensure fairness, service providers must ensure that the age verification method used has been tested on different data sets. This preliminary step is necessary for age verification methods that rely specifically on machine learning or statistical modeling. In fact, in this context, biases can occur when the data sets used to train an algorithm are not sufficiently diverse.

The UK Authority also considers it appropriate to require that, in addition to the above indicators, age verification systems be designed to ensure accessibility and interoperability.

Accessibility

To this end, the age verification system should:

a) be easy to use; and

b) work effectively for everyone.

In order to ensure accessibility, the provider must:

a) consider the potential impact that the chosen age verification method(s) may have on persons belonging to protected categories;

b) consider offering a variety of age verification methods; and

c) Design the user journey through the age verification process so that it is accessible to a wide range of abilities.

Interoperability

Interoperability describes the ability of technological systems to communicate with each other using common, standardized formats. It relies on consistent technological approaches across different systems. Standards, technical frameworks, and other specifications are important for achieving interoperability.

In the context of age verification, interoperability may involve reusing the result of an age check across multiple services by allowing different providers of age verification methods to share this information in line with data privacy laws. Service providers can take this principle into account by staying up to date with developments in this area and implementing such solutions where they exist and are appropriate for their service.

I.3 The position of the CNIL in France on the balance between child protection and privacy

In France, the CNIL (the CNIL is an independent administrative authority established in 1978 by the Data Protection Act, composed of a board of 18 members and a group of state contract agents) has analyzed the main types of age verification systems in order to clarify its

position on age verification on the Internet, and in particular on pornographic websites for which such verification is mandatory. It specifies how these publishers could fulfill their legal obligations. However, the CNIL notes that current systems can be circumvented and invasive, and calls for the implementation of more privacy-friendly models. Below is a summary of what was reported in a recent publication on its website.

Inform, raise awareness, and prioritize user control over devices

In general, the CNIL stresses the importance of informing and raising awareness among minors, parents, judicial officials, and staff in the education and youth management sectors about good IT practices, given the growing importance of digital tools in people's lives.

Therefore, as part of its work on the digital rights of minors, the CNIL published general recommendations in August 2021 setting out the requirements for verifying the age of minors and parental consent while respecting their privacy, in particular to comply with the obligations of the GDPR and the law on minors' access to social networks. Recommendation No. 7, in particular, calls for **age verification systems to be structured around six pillars: minimization, proportionality, robustness, simplicity, standardization, and third-party intervention.**

Finally, the CNIL tends to favor the use of devices under the control of users rather than centralized or imposed solutions: from this perspective, the logic of parental control, which leaves it up to families to limit access to sensitive content, seems to be the most respectful of individual rights. However, this approach has a limitation: **the law stipulates that, in certain cases, website publishers (e.g., pornographic websites) are responsible for age verification.**

The proliferation of legal obligations for online age verification

French law and certain European regulations make the provision of certain services or goods subject to age restrictions, requiring the websites concerned to verify the age of the customer: purchase of alcohol, online gambling and betting, certain banking services, etc.

In the specific case of websites that distribute pornographic content, the law of July 30, 2020, aimed at protecting victims of domestic violence, reaffirmed the obligations regarding age verification, codified in Article 227-24 of the Penal Code. The dissemination of a "pornographic message" likely to be seen by minors is therefore a criminal offense; **the law specifies that age verification cannot be based on a simple declaration by the internet user that they are at least 18 years old.**

In December 2021, the president of the Audiovisual and Digital Communications Regulatory Authority (**Arcom**), within the powers entrusted to him, **ordered several pornographic websites to establish effective age verification for internet users**.

On June 3, 2021, **the CNIL issued an opinion on the draft decree specifying, for the application of the law of July 30, 2020, the obligations of websites that distribute pornographic content**. On that occasion, it defined some fundamental principles for reconciling the protection of privacy and the protection of minors through the implementation of online age verification systems for pornographic websites:

- **no direct collection of identity documents by the publisher of the pornographic website;**

- **no estimation of age based on the Internet user's browsing history on the web;**
- **no processing of biometric data for the purpose of uniquely identifying or authenticating a natural person (e.g., by comparing, using facial recognition technology, a photograph on an identity document with a self-portrait or selfie).**

The CNIL also recommends, more generally, the use of a trusted independent third party to prevent the direct transmission of user identification data to the site or application offering pornographic content. Through its recommendations, the CNIL pursues the dual objective of preventing minors from viewing content that is unsuitable for their age, while minimizing the data collected on Internet users by pornographic site publishers.

In this context, the CNIL has issued numerous recommendations and warnings.

CNIL recommendations and warnings on online age verification

The need to regulate age verification solutions in the short term by involving a trusted third party

Age verification criteria that raise important questions

In the context of the use of a trusted third party, recommended by the CNIL in its opinion of June 3, 2021, age verification is divided into two distinct operations in practice:

- On the one hand**, the issuance of proof of age**: the establishment of a system designed to validate information about a person's age by issuing proof of age accompanied by a level of confidence. This proof can be issued by various entities that know the internet user, whether they are **service providers specializing in digital identity or an organization that knows the internet user in another context (**a merchant, a bank, an administration, etc.). Several solutions are analyzed in this document.
- On the other hand, **the transmission of such certified proof of age to the visited site** so that the latter may or may not grant access to the requested content (it should be noted that, as indicated in the PEReN note, a third step consists of analyzing the proof of age presented and granting or denying access to the requested content).

These two aspects raise important data protection and privacy issues, particularly with regard to preserving the possibility of using the Internet without revealing one's identity or directly identifiable data. **Entrusting these functions to different entities makes it possible to protect privacy in three ways**:

- The entity **providing proof of age knows the identity of the Internet user but does not know which site they are visiting**;
- The entity that transmits the proof of age to the site may know the site or service that the Internet user is visiting but does not know their identity (in the "ideal" solution developed by the CNIL, the proof of age passes through the user, which allows for compartmentalization between the actors);
- The website or service knows the age of the internet user (or only that they are of legal age) and knows that they are visiting this website, but does not know their identity and, in some cases, the age verification service used.

An independent third-party verifier to better protect people's data

In order to preserve trust among all stakeholders and a high level of data protection, the CNIL therefore recommends that websites subject to age verification requirements do not carry out age verification operations themselves, but rather rely on third-party solutions that have been independently verified for validity.

The work of the European Commission is moving in this direction, as shown in the communication entitled "A New European Strategy for a Child-Friendly Internet" (PDF), particularly in the context of the proposal for a European digital identity.

Necessary assessment of third-party age verification providers

In addition, it also seems necessary, in general, for age verification providers to be subject to third-party evaluation, especially when they adopt an approach based on automatic or statistical analysis.

To this end, and given the sensitivity of the data collected and the invasive nature of age verification systems and, more generally, the processing of identity-related information, the creation of specific labeling or certification for these third parties could help ensure that devices comply with the GDPR (respect for the principles of minimization, security of collected data, and purpose limitation).

A necessarily imperfect verification

With regard to the verification processes offered on the market, the CNIL points out that all the solutions currently available can be easily circumvented. In fact, the use of a simple VPN that locates the Internet user in a country that does not require this type of age verification can allow a minor to circumvent an age verification system applied in France, or to circumvent the blocking of a website that does not comply with its legal obligations. Similarly, it is difficult to certify that the person using the age verification is the same person who obtained it.

Thus, in the United Kingdom, where such measures have been under consideration for some time, 23% of minors claim to be able to circumvent blocking measures, and some pornographic content publishers already offer VPN services. While the use of VPNs must be subject to a certain degree of vigilance, it should be emphasized that these technologies are also one of the essential elements of secure Internet exchanges, used by many companies but also by individuals who wish to protect their browsing from tracking by public or private entities.

Analysis of existing solutions

The CNIL has analyzed several existing solutions that enable the age of online users to be verified, checking whether they have the following properties: **sufficiently reliable verification, comprehensive coverage of the population, and respect for the data protection and privacy of individuals and their security**.

The CNIL notes that there is currently no solution that satisfactorily meets these three requirements. It therefore calls on public authorities and industry players to develop new solutions in line with the recommendations set out above. The CNIL considers it urgent that more effective, reliable, and privacy-friendly systems be proposed and tested quickly. Article 3 of Decree No. 2021-1306 of October 7, 2021, entrusts ARCOM with the task of developing

guidelines detailing the reliability of the technical processes that websites must implement to prevent access by minors.

However, measures already exist to improve the level of protection for minors, particularly the youngest ones. Several solutions are described below, in descending order of maturity from the CNIL's point of view. Pending the establishment of adequate controls and only for a transitional period, the CNIL considers that some of these solutions could strengthen the protection of minors, provided that their implementation is guaranteed and, in particular, that the additional risks generated by their use are taken into account.

1. Age verification through payment card validation

Age verification via payment card has the advantage of relying solely on infrastructure that is already in place and proven. It is therefore being considered, even though this type of verification can be circumvented (as minors may have payment cards that allow them to make purchases on the Internet) and is not accessible to everyone (as adults may not have such a card, due to differences in access to credit cards depending on income). This solution is already implemented by a number of providers and is based on checking the validity of the card rather than on a payment, although some offer a micro-payment, which is immediately canceled.

Such a system makes it possible, in particular, to protect younger children (up to around secondary school age), who may not have a bank card that allows them to make online payments.

On the one hand, this age verification system should not, in principle, be implemented directly by the data controller (i.e., the website visited) but rather by an independent third party. On the other hand, the systems put in place should ensure the security of the verification in order to prevent the risks of phishing associated with it. It is therefore important to ensure that payment information is entered correctly on trusted sites. If this solution is preferred, it would be desirable for website publishers and solution providers to launch a parallel awareness campaign on the risks of phishing, taking this new practice into account in particular. Free access must remain free: the use of this system must not entail any cost to the user.

2. Age verification through facial analysis

Some age estimation processes are based on facial analysis, but do not aim to identify the person. However, those who contest the outcome of the verification must have another method of verification available.

The use of such systems, due to their intrusive nature (access to the user's device camera during initial registration with third parties, or random checks by these same third parties, which could be a source of blackmail via webcam when requesting access to a pornographic site), as well as the margin of error inherent in any statistical assessment, should be subject to compliance with reliability and performance requirements independently verified by a third party.

According to the CNIL, age estimation carried out locally on the user's terminal should be preferred in order to minimize the risk of data leakage. In the absence of this requirement, this method should not be used.

3. The offline verification system

The most successful offline verification method appears to be the sale of scratch cards to adults only, which allow them to obtain an identifier and password that would give them access to age-restricted content. These cards would be offered at certain points of sale, such as supermarkets or tobacco shops, where employees already carry out age checks in connection with the sale of alcohol, cigarettes, and gambling.

However, this mode cannot be used exclusively for viewing pornographic sites, as this could be stigmatizing for the person concerned. All activities subject to age restrictions should be included, and this model should be promoted by a diverse community of publishers (purchases of regulated products, pornography, etc.). The limitations of such a system would be the same as those for purchasing cigarettes or alcohol, namely fraud through the resale of cards on a parallel market.

Prerequisites: this method requires specific governance, with an authority that issues the cards and manages the authentication systems.

4. Age verification through identity document analysis

Age verification can be carried out by a third party responsible for collecting and analyzing an identity document provided by the user. This system can be easily circumvented by using another person's identity document if only a copy of the document is required (it is possible to use another adult's document, even within the same household). This system is therefore unreliable and disrespectful of personal data, because it requires the collection and processing of official identity documents in order to function.

Some systems verify a person's identity by comparing the photograph on the identity document provided with a "live detector" test, i.e., capturing a photograph or video of the user at the time of the required age verification, in order to verify that the user is indeed who they claim to be and to combat possible circumvention of the device. This process is much more reliable and is also used for identity verification in accordance with the ANSSI PVID standard.

However, as it involves the processing of biometric data, its use should be particularly regulated and, in principle, in accordance with the GDPR, be provided for by a specific legal provision or based on the free consent of individuals.

Prerequisites: as with the PVID standard, a certification (or labeling) body must be established to verify that the necessary safeguards are in place for the collection and analysis of identity documents.

5. Using government tools to verify identity and age

The use of public databases or an authentication system such as FranceConnect could theoretically make it possible to prove one's age in order to access certain websites or online services. However, FranceConnect was not designed for this purpose, but rather with the aim of simplifying administrative procedures: its very functioning is based on the recording of usage on government servers. This method therefore does not appear satisfactory, as it would lead the government to

have a list of purely private connections. Furthermore, with regard to the consultation of pornographic sites, the use of these devices would carry the risk of associating an official identity with intimate information and a presumed sexual orientation.

On the other hand, as explained above, the connection of an attribute management service operated by a trusted third party to the state's identity systems could be considered.

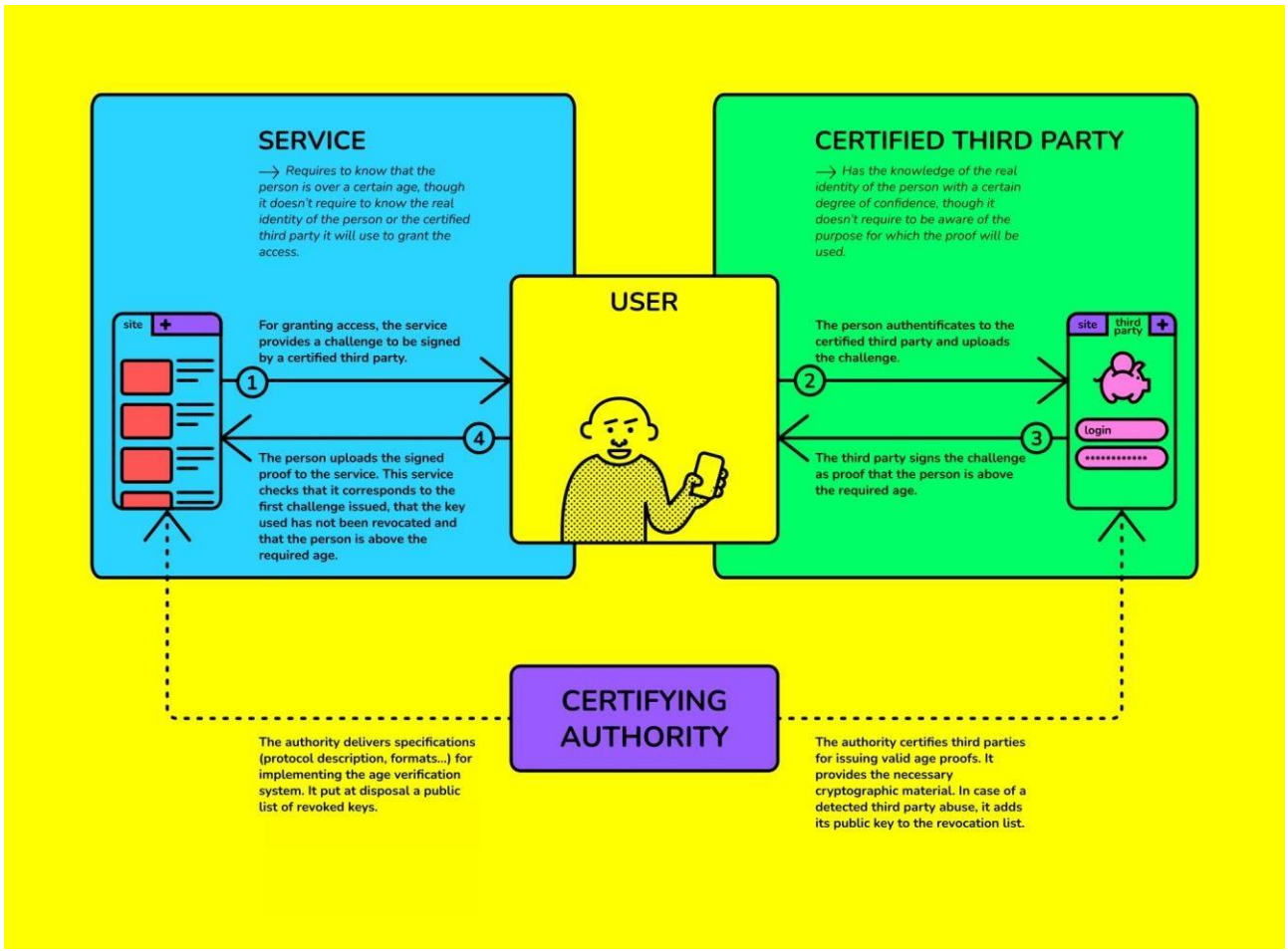
Prerequisites: it is necessary to use trusted third parties to link attribute management services to state identity systems.

6. Inferential age verification systems

There are three main variants of this type of analysis: the first appears to be difficult to reconcile with data protection, while the second raises questions of reliability. The third, which also raises important questions, can only be used by a limited number of services that already collect a lot of browsing data.

- Importing an individual's internet browsing history: this method appears too intrusive for the simple purpose of age verification.
- Analysis of "maturity" using a questionnaire: this method seems to avoid the transfer of personal data. However, this method appears to be relatively reliable and the possibility of circumvention (sharing answers online) is significant, as are the biases that could be associated with it. For example, part of the population could be discriminated against based on their skills (reading, comprehension), their level of language proficiency, their cultural references, etc. This method should therefore be avoided.
- Analysis of browsing on the specific services of the website publisher (in particular large digital platforms). The reuse of data for the creation of age inference (or deduction) models seems possible, subject to the following points:
    - in principle, this method should not lead to an automated decision, but to an initial estimate which, in the event of suspected non-compliance with the age requirement, may lead to an exchange with the internet user;
    - no additional data should be collected for the sole purpose of building the model (only data already collected should be used);
    - The data produced on the platform's services must be distinguished from data collected by tracking user navigation on other sites (e.g., through authentication on the platform, through the installation of a mechanism to track access to certain web pages, etc.).
    - the inference system should be evaluated by an independent third party in order to limit risks.

The CNIL's Digital Innovation Laboratory (LINC) has demonstrated the feasibility of a system based on a secure protocol, which relies on a process implemented in cryptography that allows identified individuals to prove that a situation is true without having to reveal other information. It has been shown that it is possible, through a third-party system, to guarantee the protection of the individual's identity and the principle of data minimization, while maintaining a high level of assurance regarding the accuracy of the data transmitted. However, this assumes that the third parties used are completely independent of the publishers.



I.4 Public consultation by the French regulator Arcom

In France, pursuant to the provisions of Article 227-24 of the Criminal Code, introduced by Law No. 92-684 of July 22, 1992, it is prohibited to expose minors to pornographic content. Article 23 of Law No. 2020-936 of July 30, 2020, aimed at protecting victims of domestic violence, entrusted the Regulatory Authority for Audiovisual and Digital Communications (Arcom) with the prerogative to issue warnings to public communication services that do not comply with this criminal obligation, as well as to refer them to the courts in order to block sites that do not comply with the aforementioned warning.

The French bill known as PJL SREN, aimed at securing and regulating the digital space, provides for Arcom to be given the power to administratively block online public communication services with editorial responsibility and video-sharing platform services that disseminate pornographic content accessible to minors after they have been ordered to comply with Article 227-24 of the Criminal Code. This power, exercised under a special procedure supervised by the administrative court, would supplement the powers otherwise granted to the judicial court in this area.

In addition, the bill provides that **Arcom shall adopt a framework, after consulting with the National Commission for Information Technology and Civil Liberties (CNIL), to determine the minimum technical requirements applicable to age verification systems set up for access to services that distribute pornographic content.** Failure to comply with the requirements shall result in a financial penalty, following a warning from Arcom.

On April 11, 2024, Arcom published a **public consultation on the draft framework determining the minimum technical requirements applicable to age verification systems put in place for access to online pornographic content**, in anticipation of the adoption of the PJL SREN bill.

The text submitted for consultation provides for a set of mandatory minimum requirements and optional requirements as described below.

Robustness of the solution

The protection of minors must be the default setting, starting from the display of the first page of a public online communication service that allows the dissemination of pornographic content. Online services that transmit pornographic content are required to display a screen that does not contain pornographic content "unless the user's age has been verified."

Online services that transmit pornographic content must ensure that no user accesses pornographic content until they have proven that they are of legal age, for example, by completely obscuring the service's home page.

Publishers can indicate the pornographic nature of their service. To do so, they can rely on a self-declaration mechanism (e.g., labeling each web page as "restricted to adults"), allowing parental control systems to be aware of the minimum age required to access the site's content.

Effectiveness of the solution

The technical age verification solution implemented by services distributing pornographic content must allow for a clear distinction between underage and adult users.

Limiting the possibility of circumvention

Services that distribute pornographic content must do their utmost, in accordance with the high standards of professional diligence in the industry, to limit the possibility of circumventing the technical solutions they implement. Age verification systems must not allow proof of age to be shared with other people. Finally, the system must be robust against the risks of attacks, such as *deepfakes*, *spoofing*, etc.

For example, with regard to solutions based on age estimation through facial feature analysis, services that transmit pornographic content must ensure that the solutions contain a mechanism for recognizing living organisms, the effectiveness of which complies with the state of the art. Detection must be carried out with sufficient image quality and must exclude any diversion process that could be used by minors to artificially appear as adults, in particular through the use of photos, recorded videos, or even masks. On the other hand, with regard to technical solutions for generating proof of age based on the presentation of a physical identity document, the services concerned that distribute pornographic content must verify: (i) that the document is genuine and not a simple copy; (ii) that the user is the holder of the identity document provided. This verification can be carried out in particular by recognizing facial features using a live detection mechanism, under the conditions indicated above.

Age verification each time the service is accessed

Age verification must take place each time a service that disseminates pornographic content is accessed. After access to the service is interrupted, a new age verification must be triggered in the event of renewed access to pornographic content.

Compliance with this criterion does not preclude the possibility for the user to use reusable or self-regenerated proof of age, provided that a second authentication factor is present. This can be done by linking the use of reusable proof to the terminal of the person concerned, as in the case of digital wallets. Furthermore, the verification system must not allow this proof to be shared with another person or service.

For example, in the case of a device shared between an adult and a minor, it is advisable to ensure that the validity period of the age verification does not allow the viewing of pornographic content without further verification. The validity of an age verification must therefore cease when the user exits the service, i.e., when the session ends, when the user exits the browser, or when the operating system goes into standby mode, and in any case after a period of one hour of inactivity.

Use of a user account

The implementation of an age verification solution must not require the creation of a user account on the service in question that makes pornographic content available. Furthermore, proof of age cannot be stored in a user account on that service. In any case, the age verification requirement applies to every access, with or without a user account.

Non-discrimination

The solutions adopted by targeted services that disseminate pornographic content must not have the effect of discriminating against certain groups of the population, in particular on the grounds set out in Article 21 of the Charter of Fundamental Rights of the European Union. Therefore, the effectiveness of the technical age verification solution must be the same regardless of the physical characteristics of the user. With regard to age verification systems based on *machine learning or* statistical models, service providers may, for example, test their solution on different databases to ensure compliance with this requirement.

It is essential that age verification systems limit discriminatory biases, which also generate errors that call into question both their reliability and acceptability.

Online services that disseminate pornographic content are invited to integrate any discriminatory biases, broken down by relevant grounds of discrimination, into the performance assessment of their age verification system, but also during audits.

Protection of personal data

Age verification systems as a whole must comply with current legislation on the protection of personal data and privacy, including the principles of data minimization and data protection by design and by default (Articles 5 and 25 of the GDPR).

Providers of such systems must pay particular attention to the following principles:

- accuracy, proportionality, and minimization of the data collected;
- concise, transparent, understandable, and easily accessible information for users;
- appropriate data retention periods;
- the possibility for data subjects to exercise their rights, namely the right of access, the right to object, the right to rectification, the right to restriction of processing, the right to erasure, and the right to portability;
- state-of-the-art security for information systems used in the processing of personal data.

In 2022, the CNIL published an example of a privacy-friendly age verification mechanism for the transmission of an identity attribute (in this case, proof of age). This mechanism, known since then as "double anonymity" or "double confidentiality," has been developed and tested by various public and private actors, allowing them to

confirm its technical feasibility and its ability to meet the need for privacy protection inherent in online age verification mechanisms. It also corresponds to the objectives generally set for digital identity systems, including attribute management. However, this mechanism, although called "double anonymity," is not entirely "anonymous" within the meaning of the GDPR, but it does guarantee a high level of confidentiality.

Public online communication services that make pornographic content available must offer their users at least one age verification system that complies with 'double anonymity' privacy protection standards, ensuring that this system can be used by the vast majority of its users.

This requirement will come into force at the end of the transitional period provided for in the regulation, without prejudice to the minimum requirements set out below. Therefore, until that date, age verification systems must comply with the minimum basic requirements set out below to ensure an acceptable level of protection of their users' personal data.

Minimum requirements applicable to all age verification systems

The following criteria constitute a minimum set of requirements applicable to all age verification systems covered by the proposed regulation.

Independence of the age verification system provider from the targeted services disseminating pornographic content

The provider of age verification systems must be legally and technically independent from any online public communication service covered by the regulation and ensure that the services concerned that disseminate pornographic content do not have access to the data used to verify the user's age under any circumstances.

Confidentiality with regard to services disseminating pornographic content

Personal data enabling users to verify their age with a communication service covered by this proposed regulation must not be processed.

In particular, the implementation of age verification solutions must not allow communication services covered by the regulation to collect the identity, age, date of birth, or other personal information of such users.

Confidentiality with regard to providers generating proof of age

Where the age verification system does not allow the user to obtain a digital identity or reusable proof of age, the personal data provided by the user to obtain age verification should not be stored by the age verification service provider. Furthermore, this type of system should not require the collection of official identity documents.

Confidentiality towards any other third parties involved in the age verification process

Where third parties other than age verification providers are involved in the age verification process, for example for the management of the verification or billing of the service, such third parties shall not retain the personal data of the system users' staff, except for the storage of the verification at the user's request.

Measures to safeguard the rights and freedoms of individuals through age verifiers

When determining whether a user can access a public online communication service based on the evidence presented to them, the service concerned that disseminates pornographic content shall take

an automated decision within the meaning of Article 22 of the GDPR. In fact, by refusing access to a service, this decision is likely to produce legal effects on the data subjects, or at least to produce significant effects that affect certain individuals in a similar way.

The CNIL considers that this decision may be based on the exception provided for in paragraph 2.b. of Article 22 of the GDPR, insofar as the service in question, which disseminates pornographic content, is subject to the age verification requirement provided for in Article 227-24 of the Criminal Code and, ultimately, by the provisions of the PJL SREN. Article 22.2.b of the GDPR requires that appropriate measures to safeguard the rights, freedoms, and legitimate interests of the data subject be provided for in the provisions authorizing such automated decision-making.

In order to preserve privacy requirements that aim to limit the ability of services to identify individuals, these measures must be implemented not by the service in question that disseminates pornographic content, but by the provider of the technical solution for age verification, regardless of the provider of the attribute or the issuer of the proof. Such measures must allow users, in the event of an error, to challenge the result of the analysis of their characteristics in order to obtain proof of age. To exercise these remedies, age verification solution providers should offer users the option of using different attribute providers or, depending on the solution, different proof issuers.

The service in question that disseminates pornographic content is still required to comply with the information obligations imposed by the GDPR and must notify users of the possibility of using the age verification solution provider.

In any case, attribute providers must also allow individuals to rectify their data in accordance with Article 16 of the GDPR.

Enhanced confidentiality for targeted services that disseminate pornographic content

An age verification system that uses "double anonymity" must not allow communication services covered by the regulation to recognize a user who has already used the system on the basis of data generated by the age verification process.

The use of age verification systems that use "double anonymity" should not allow these services to know or infer the source or method of obtaining age evidence involved in a user's age verification process.

An age verification system that complies with "double anonymity" should not allow these services to recognize that two pieces of evidence of age come from the same source of age evidence.

Enhanced confidentiality for individuals providing proof of age

An age verification system that uses "double anonymity" must not allow age proof providers to know for which service the age verification is being performed.

Enhanced confidentiality for any other third parties involved in the age verification process

An age verification system that uses "double anonymity" must not allow any other third party involved in the process to recognize a user who has already used the system. For example, a third party that ensures the transmission of age proof or certifies its validity must not be able to know whether it has already processed proof from the same user.

Availability and coverage of the user population

Regulated communication services must ensure that their users have at least two different methods of generating proof of age, allowing them to obtain proof of age through a "double anonymity" age verification system. In practice, a service provider offering a double anonymity solution must combine at least two methods of obtaining proof of age (e.g., a solution based on identity documents and a solution based on age estimation).

Communication services covered by this standard must ensure that a "double anonymity" age verification system is available to at least 80% of the adult population residing in France.

Explicit information on the level of user privacy protection

Each age verification solution must be explicitly associated with its level of privacy protection, so that solutions that meet "double anonymity" standards are clearly and legibly displayed. In any case, other solutions must not be confused or highlighted in order to mislead the user in favor of solutions that offer less privacy protection.

If a third party involved in the age verification process becomes aware of the service for which age verification is being carried out, the user must be clearly informed.

For age verification systems that comply with the principle of "double anonymity," the user must be clearly informed that this solution ensures that the age verification provider cannot know the service for which the verification is being carried out.

Non-mandatory requirements and good practices

The following criteria are not currently mandatory for age verification systems, but constitute a set of good practices that age verification solutions should aim for.

Ability for the user to independently generate proof of age confidentially:

- the user can generate proof of age locally, without informing the initial issuer of their age attributes or any other third party;
- the user can generate proof of age via an online service that can be used without having any access to their personal data.

Confidentiality of age verification systems as a whole:

- the system is based on zero-knowledge proofs;
- the system is based on encryption techniques with properties that resist even the most complex attacks, including future ones

Temporary derogations for evidence generation accepted

The French regulator stipulates that, for a transitional period of six months from the publication of the regulation, intended to allow the services subject to it to identify and implement an age verification solution that meets all the criteria determined, solutions using bank cards will be deemed to comply with the technical characteristics of the framework, subject to compliance with the following conditions.

A solution using bank cards would be an initial way of filtering out some minors.

Filtering can be carried out either in the form of a €0 payment or through simple authentication (without payment).

These verification systems:

- must not be implemented directly by the targeted services that distribute pornographic content, but by a third party independent of the service;
- must guarantee the security of the verification in order to prevent the risks of phishing associated with it. It is therefore important to ensure that payment information is entered correctly on trusted sites. In this regard, it would be desirable for targeted services that distribute pornographic content and solution providers to launch a coordinated awareness campaign on the risks of phishing, taking particular account of this new practice;
- they must at least allow the existence and validity of the card to be verified, excluding a simple check of the card number;
- implement the strong authentication required by European Directive (EU) 2015/2366 on payment services (known as "PSD2"), for example by relying on the 3-D Secure protocol, in its second version currently in force, to ensure that the service user is the cardholder through two-factor authentication.

At the end of this transitional period, Arcom will again specify the conditions under which age verification by bank card may continue to be accepted.

I.4 Public consultation by the Spanish regulator

The Spanish regulatory authority (CNMC) has launched a *public consultation on the criteria for ensuring the adequacy of age verification systems on video-sharing platforms for content harmful to minors.*

In the national regulatory context, Spanish Law 13/2022 of July 7 on general audiovisual communication (*Ley General de Comunicación Audiovisual*; hereinafter LGCA) extended the subjective scope of regulated entities, audiovisual media service providers, to include video-sharing platform service providers. The purpose of this extension is to ensure the protection of minors from harmful content, as well as to protect users in general from content that incites violence, hatred, or the commission of a crime, particularly terrorism.

Article 89 of the LGCA imposes a series of obligations on these new agents, **including the obligation to implement age verification systems for access to their platforms**, as a gold standard measure to protect minors from harmful audiovisual content.

The consultation in question aims to ensure that the implementation of this new rule is as effective as possible.

The regulator notes that the existence of freely accessible and unrestricted VSPs (video sharing platforms) aimed at disseminating content that is inherently harmful to minors, such as violence or pornography, is a matter of social concern. This is particularly true when such content is made accessible to minors, as it can alter their understanding and compromise their physical, mental, or moral development. In this context, it highlights that the development of the new European regulatory framework for audiovisual media has included the obligation for VSPs to establish measures to ensure the protection of minors and, in particular, measures to prevent minors from accessing particularly harmful content. These obligations have been transposed into Spanish law through the LGCA of July 7, 2022.

In this context, the consultation aims to indicate the minimum and essential elements that age verification systems must have in order to be considered compliant with the objective set out in the LGCA.

On the material scope of the obligation to establish and operate age verification systems to prevent access by minors

The LGCA mentions two cases in which age verification systems would be applicable.

On the one hand, Article 89.1.e) of the LGCA provides that VSPs must "Establish and manage systems for verifying the age of users with respect to content that may compromise the physical, mental, or moral development of minors, which, in any case, prevent minors from accessing the most harmful audiovisual content, such as gratuitous violence and pornography." Considering that the advertising offered by these providers encourages behavior that is equally harmful to minors, since in many cases it refers to pornographic sites, drugs of dubious origin, violent or sexually explicit video games, dating sites, or direct contact telephone numbers for sexual services, it is considered justified that the obligation to establish and operate age verification systems should apply to all audiovisual content, including commercial communications managed by VSPs subject to Article 89(1)(e).

I. On the minimum elements of age verification systems that prevent access by minors

Based on an analysis of the various age verification services, as well as the experience of France and Germany, the regulator proposes a set of minimum elements that the various age verification systems must meet in order to be considered compliant with the law.

- The age verification system implemented by the VSP must ensure, at all times, that the person accessing harmful content is of legal age.

  Given that access to this type of service tends to be recurrent, it will be necessary to ensure that the person who initially certifies their age is also the only one who can use that certification to access the service in the future.

  In other words, the verification system must ensure that the person who wants to access the content is actually the person identified as an adult, avoiding possible cases of identity theft or system violation.

  Identification and authentication can be carried out on the basis of **identity documents or digital certificates.** In some cases, prior registration is possible, where the age of the registrant is identified, and subsequent verification that the person (previously identified) is the one authenticating themselves to access the service.

  Age verification mechanisms will consist of two stages: the first corresponds to the unique identification of the person, the second to an authentication confirming that it is the previously identified person accessing the adult service on each subsequent use.

- The first step in unique identification involves the necessary personal identification with age verification.

  To collect identification and age verification data, it has traditionally been necessary to carry out a *face-to-face* check and use official identity documents (national identity card, residence permit, passport), comparing the photograph or fingerprint.

national identity card, residence permit, passport), comparing the photograph or fingerprint.

However, technological advances in the development of this type of solution seem to make **face-to-face checks unnecessary when using digital identity mechanisms**, provided that such verification avoids the risk of falsification and circumvention.

In any case, it is up to the provider to decide which age verification mechanisms to implement for their service and, ultimately, it is up to each user to choose from the options offered to them.

The regulator considers it reasonable **to reject as inadequate certain solutions such as the simple presentation or sending of a copy of an identity document, as well as identification and age verification by means of a photograph**, as these do not provide adequate guarantees.

Finally, it is necessary to ensure that access keys are only transmitted to the identified person.

- The second stage of authentication consists of ensuring that only the identified and age-verified person has access to the service in question.

  To this end, authentication must take place at the beginning of each usage or login process, and access to content must depend on an individually assigned authentication element. Furthermore, since in most solutions, after unique identification, the user, recognized as an adult and therefore authorized, receives a form of "password" for all subsequent usage processes, it is necessary to prevent the possibility of transferring access authorizations to unauthorized third parties. The disclosure or multiplication of passwords can be prevented by technical measures that make it difficult to multiply access authorizations, but also by informing the user of the personal risks arising from the unauthorized use of their password.

The system must be robust and accurate to prevent possible identity theft.

Regardless of the type of identification used, it is essential that the criteria applied ensure that the person identified is of legal age.

Technological neutrality

Given the various ways of accessing pornographic, violent, and other harmful content, the age verification system should be usable on any technological device and operating system, so that minors cannot circumvent or bypass controls and access content.

II. The technological solutions available for age verification

The regulator believes that simply declaring that one is of legal age without any subsequent verification does not provide an adequate level of security to prevent minors from accessing such content. There are currently age verification solutions on the market that could be effective. The validity of a technological solution for age verification depends on how reliably it prevents minors from accessing content, without prejudice to compliance with personal data protection legislation. Technical solutions can be broadly grouped into

two types. The main features of each will be illustrated below, specifying, where appropriate, the possible disadvantages of each.

A. Age verification using an identity card or digital certificate derived from it

- Age verification can be carried out by checking a traditional physical **identity document**, an electronic physical identity document, or a digital identity document. These documents could be, for example, identity cards, passports, residence certificates (EU citizens), residence cards (non-EU citizens), or a digital or virtual identity medium not based on a physical document.
- Similarly, as an alternative to actual identity, it is possible **to use credentials confirming that the user has reached the age of majority,** such as those provided for in the eIDAS Regulation, soon to be adopted, based **on digital identity**. In this way, the legal age can be independently verified without the need to disclose further information about the user, in accordance with the principle of minimization and preserving the user's anonymity.

  With regard to authentication, *face-to-face* or remote procedures based on keys, fingerprints, or photographs of the person could be used.

  Some authentication solutions require the face to be brought close to the camera of the device used to request age verification, to ensure that a photograph is not being used.

  In face-to-face solutions, adults **can obtain adult-only cards, which give** them **a username and password** that would allow them to access age-restricted content. These cards would be offered at certain points of sale, such as supermarkets or tobacco shops, whose staff are familiar with age checks for the sale of alcohol or cigarettes. The main disadvantage is that such a measure introduced only for viewing pornographic or violent sites could stigmatize the person concerned and discourage them from using it. Another disadvantage would be the resale of cards on a parallel market.

  Each of these mechanisms could be implemented via apps for the most common smartphone operating systems, which facilitate identification and authentication. This structure could be a feature **of digital identity wallets**.

  As noted above, it is ultimately up to the user to choose one mechanism or the other.

B. Age verification via bank card

In existing solutions of this type, users enter their name and bank card details (card number, expiry date, CVC code) and this data is compared with a payment database to verify that the card is valid. This may be a simple check that the number provided is in the correct format, a request for pre-authorization of a payment, or a micro-payment to obtain the highest level of certainty.

In general, this system protects younger children (under 10-12 years old) who do not have a bank card that allows them to make online payments and who are less likely to use third-party cards. The disadvantage of this solution is that it offers a lower level of security, as minors may have bank cards that allow them to make purchases on the Internet. Another disadvantage is that bank cards

may not be accessible to everyone, as they are usually linked to a certain income level.

III. On organizations that could carry out age verification

Age verification can be carried out by the provider itself or by an independent third party. The latter case has certain advantages for the provider, such as the outsourcing of a service that can be complex to perform, but above all, it does not discourage the use of services by adults who are more reluctant to provide their data to VSPs.

In this sense, independent age verification organizations can also be used to purchase alcohol or tobacco or to allow online gambling. In addition to the above examples for proof of legal age, third-party verifiers are widely used by telecommunications companies and banking organizations to validate their customers' data before entering into online contracts.

In this way, the third party providing proof of age knows the identity or age attribute of the internet user, but does not know which site they are visiting, and the service provider knows that the user is of legal age, but does not know any other personal or identity-related information about the user. It is necessary to clarify that the user must know whether the third party is independent of the service provider to which they are requesting access and be aware of any possible economic links between third parties and service providers.

IV. On further aspects to be satisfied through age verification

Additional aspects related to the security of age verification mechanisms must be considered, such as the existence of backdoors, the maximum duration of a session, or the time limit for considering inactivity. Another aspect to consider among all the options available on the market for age verification is choosing a service that adequately collects age data in the least invasive way possible, respecting people's privacy.

V. Summary of contributions to the public consultation

In April 2024, the National Commission on Markets and Competition (CNMC) published a summary of the contributions[19]to the public consultation on age verification systems used by video platforms in Spain to prevent minors from accessing harmful content (INF/DTSA/329/23). The CNMC, in accordance with the General Audiovisual Communication Law, has the power to assess whether the systems used by video platforms established in Spain prevent minors under the age of 18 from accessing harmful content—pornography and gratuitous violence—when verifying the age of its users.

During the public consultation process, 35 contributions were received from virtually all stakeholders in this sector: user associations, media, audiovisual agents, age verification system providers, verifiers, and video exchange platforms (PIVs).

Scope of the access ban

All responses agree that age verification systems (AVS) must cover both content and related advertising, as these also violate the rights of minors. With regard to the type of platform that must have AVS, the vast majority (61.5%) believe that AVS should take precedence over pornographic content, regardless of whether it is

[19] https://www.cnmc.es/prensa/respuestas-cp-verificacion-edad-plataformas-20240417

hosted on a generalist or pornographic platform, and that the EAV should be applied before access to content (65%), regardless of the type of platform.

Freedom in the choice of age verification systems

Most contributions (83%) argue that there should be several EASs and that the platform should choose which one to implement. This approach not only benefits platforms, which can choose the EAS that suits their business model, but also responds to the different needs of users (varying degrees of technological knowledge, lack of an official document, or reluctance to share it).

Age verification systems available on the market

Most agents opt for remote or non-face-to-face verification (85%), and the two main options in the industry are:

1. Verification via ID document and photo comparison (selfie)
2. Age estimation through facial analysis.

Balance between system suitability and data protection

The majority believe that data protection is a determining factor in the effectiveness of the EAV. Anonymity in accessing content was highlighted by several agents and, in line with this, the European digital wallet (eIDAS2) was indicated as ideal for this process, as it allows only the age of majority to be validated without sharing more data.

On the other hand, a significant number of stakeholders support the EAS proposal of the Spanish Data Protection Agency. Other stakeholders argue that facial estimation systems are suitable for this process.

Third parties that could carry out age verification

92% prefer an independent third party. This option is based on the fact that there are already verification agents on the market that perform this function securely, in compliance with data protection and with transparency for the user. Furthermore, having the verification carried out by a third party generates trust among users.

Self- and co-regulation tools

81% understand that this can be a very useful tool as it involves the industry, allows for greater flexibility and speed of adaptation to change, and can also contribute to the creation of standards. On the other hand, this system is perceived as slow to build.

I.5 German regulation

In May 2022, the German regulatory authority Kommission für Jugendmedienschutz (KJM) established criteria[20] for the evaluation of age verification systems.

[20] KJM website for age verification systems https://www.kjm-online.de/aufsicht/technischer-jugendmedienschutz/unzulaessige-angebote/altersverifikationssysteme

These are based on the concept that certain pornographic content that is harmful to minors may only be distributed on the Internet if the provider ensures that only adults can access it by means of so-called age verification systems (AV systems).

The requirements for such AV systems are significantly higher than the technical requirements for general access to content, as they must ensure that age verification is carried out by means of personal identification.

The KJM has therefore developed an **evaluation process** with which it analyzes and evaluates age verification systems at the request of companies or providers, possibly with discussions or on-site audits. However, the primary responsibility for implementing a verification system that complies with the criteria lies with the content provider. The latter must ensure that pornographic content and other content harmful to minors in its offering is only accessible to adults (closed user groups).

Details of the evaluation grid are published in the document "Criteria for the evaluation of concepts for age verification systems"[21].

According to the KJM criteria, age verification for closed user groups must be ensured through two closely interlinked steps:

a) through **at least one-time identification** (age verification), which must generally take place through personal contact. The prerequisite for reliable verification of legal age is the personal identification of natural persons, including verification of their age. Personal identification is necessary to avoid the risk of forgery and circumvention.

b) through **authentication during individual usage processes**. Authentication serves to ensure that only the identified person whose age has been verified can access closed user groups and to make it more difficult to pass on/transfer access authorizations to unauthorized third parties.

There are additional security requirements for age verification systems, such as protection against *backdoors*, session time limits, timeouts after a certain period of inactivity, etc.

The KJM assessment grid enables transparent processes for providers and covers the following cases:

1. **Age verification concepts for one-time use (single-use key)**

   As a method of age verification, which is always performed immediately before each use or each access, it is acceptable, for example, to use age confirmation via the eID function of the identity card.

   In addition, procedures that determine with a high degree of probability that the user is of legal age (plausibility check) may be sufficient. In contrast to reliable age verification concepts for repeated use (see below), the entire procedure must be performed each time the card is used.

   This can be achieved, for example, through a procedure in which the user is examined **via a webcam**, provided that only appropriately trained personnel are used, effective *live* detection is carried out, and sufficient image quality is ensured. Liveness detection and sufficient image quality

[21] KJM criteria for age verification systems published online at the following link (in German) https://www.kjm-online.de/fileadmin/user_upload/KJM/Aufsicht/Technischer_Jugendmedienschutz/AVS-

are necessary to ensure that a real person is sitting in front of the camera and to rule out possible circumvention, e.g., the use of recorded footage or masking. If the user is not clearly of legal age, an additional identity check must be carried out. If the identity check is carried out via webcam, the above requirements also apply in this case.

It is also necessary to ensure that **the ID card** is checked on all sides and in its entirety. If it cannot be established with certainty that the user is of legal age, access may not be granted.

However, simply verifying the ID card number or presenting a copy of one's ID document is not sufficient. Even a certified copy of an ID document is not sufficient, as it only confirms that a document matches, but does not identify a person.

2. Concepts of age verification for repeated use (general key)

Age verification for repeated use consists of two steps: identification and one-time authentication of the identified person for each session of use. After one-time identification, the user who is recognized as an adult and therefore authorized is assigned a kind of "general key" for all subsequent usage processes. This gives them access to any number of different offers. Compared to the previous "single-use key," an age check carried out simply by visual inspection of the person does not meet the requirements in this case.

The prerequisite for a reliable method of verifying age is the identification of natural persons. Personal identification is necessary to avoid the risk of forgery and circumvention.

The KJM requirements for **identification** are specified as follows:

A. Identification of the natural person: The identification of the persons concerned must generally take place at least once **through personal contact**, i.e., a facial check of those present ("face-to-face" check) with a comparison of official identification data (ID card, passport).

   Under certain conditions, it is also possible to use a "face-to-face" check that has already taken place. This is the case, for example, with identification procedures using verified personal data, such as age or date of birth, which are used when using certain services or entering into certain contracts (e.g., mobile phone contracts, opening bank accounts, etc.).

   Facial checks among those present ("face-to-face" checks) are not necessary if identification is carried out using **software that compares the biometric data on the identity document** with a photo of the person to be identified and automatically records the data on the identity document.

   Face-to-face checks of those present can be waived by comparing official identification data (ID card, passport) if an age verification procedure based on automated age determination via camera is used. The software makes statements about the probability of the age of the person to be identified based on the biometric characteristics of a live camera image and thus achieves the level of reliability of a personal age check.

B. Collection and storage of data necessary for identification: The personal data of the person to be identified that is necessary for age verification should be recorded and stored to the extent necessary in compliance with data protection regulations (e.g., date of birth, name, address).

C. Requirements for collection points: Identification data can be collected at various locations (e.g., post offices, various retail outlets such as mobile phone stores, lottery outlets, banks, and savings banks, etc.). As an alternative to forwarding the data to the AVS provider, it is also sufficient to transmit only a reference to the recorded data (storage location, specific location).

D. Final age check: Access to the closed user group (activation of user data for authentication) can only take place if the AVS provider receives the identification data or a reference to it and verifies the age.

Finally, with regard **to authentication**, which is intended to ensure that only the identified and age-verified person can access closed user groups and to make it more difficult to transfer access authorizations to unauthorized third parties, the requirements stipulate:

A. Performing authentication at the beginning of each usage process ("session");

B. Protecting content with a special password assigned individually.

I.6 The Irish regulator's public consultation

The Coimisiún na Meán (hereinafter referred to as the Commission) is the Irish regulatory body for broadcasting, video on demand, online safety, and media development. Among other things, it is responsible for setting standards, rules, and codes for the various types of media services and related online services under Irish jurisdiction.

On December 8, 2023, the Commission launched a public consultation[22] proposing an "Online Safety Code" for services and video sharing platform providers (hereinafter "VSPS" or "VSPS providers").

Online Safety Code proposed by the Irish Commission

One of the Commission's main tasks is to develop an online safety code for services provided by video sharing platforms. A VSPS is a type of online service where users can share videos and interact with a wide range of content and social features.

In accordance with its statutory powers and in compliance with its statutory duties, the Commission has prepared a draft Online Safety Code with the aim of ensuring that VSPS providers take appropriate measures to protect minors from harmful content, including illegal and age-inappropriate content. It also aims to protect the general public from content such as incitement to violence or hatred, incitement to commit a terrorist offense, the dissemination of child pornography, crimes of racism or xenophobia, as well as certain advertisements and communications.

Within the Code, the Commission has specified some important definitions to frame the context so that the obligations imposed on VSPS providers allow for the adoption of measures

[22] Available online at https://www.cnam.ie/wp-content/uploads/2023/12/Draft_Online_Safety_Code_Consultation_Document_Final.pdf

to provide adequate protection against possible harm to minors, as defined by the AVMS Directive:

Age verification techniques

VSPS providers are required to take effective measures to verify or estimate age and to establish a mechanism to assess their effectiveness.

In some cases, robust age verification (and an equivalent mechanism to assess its effectiveness) is necessary. Providers are required to report on the effectiveness of the mechanisms they have put in place. **The Commission considers that the Code should refer to the effectiveness of age verification methods rather than specifying particular techniques to be used.**

This is to give VSPS providers some flexibility in designing techniques appropriate to their particular service and in modifying them as technology develops. In addition, providers must be transparent about the age verification techniques they use and their targets for the percentage of minors who are incorrectly assessed as adults.

With regard to **age verification techniques,** the Online Safety Code developed by the Commission requires video-sharing platform service providers to implement effective measures to ensure that content classified as unsuitable for children cannot normally be viewed by children.

These measures will be applied at the time of registration for the service or each time such content is accessed and may be achieved by using age estimation or age verification, as appropriate, or by other technical measures.

Self-declaration of age by users of the service does not in itself constitute an effective measure.

In particular, providers of video-sharing platform services whose main purpose of the service or a section thereof is to provide adults with access to:

- content consisting of pornography, or

- content consisting of realistic depictions of the effects of serious or gratuitous violence or acts of cruelty,

They must implement thorough age verification techniques both for registering an account with the service or accessing the section of the service that provides access to such content, and each time such content is accessed.

In particular, such providers must establish a mechanism to describe the age verification technique used, describe how the measures are used to restrict access to the service(s), set targets for the number of minors (in different age groups determined by the service provider) who are incorrectly identified as adults through the service provider's age verification mechanisms, and assess the accuracy and effectiveness of the robust age verification systems implemented.

With regard to personal data, the Code requires video-sharing platform service providers to ensure that the personal data of minors collected or otherwise generated by them in the implementation of age verification obligations is not processed for commercial purposes, such as direct marketing, profiling, and targeted behavioral advertising.

Age verification covers a range of technical measures to estimate or verify the age of children and users, including:

- technical design measures;
- self-declaration;
- age verification using tokens via third parties;
- Systems based on artificial intelligence and biometrics;
- rigid identifiers such as passports.

The Code requires that age verification techniques be used that are effective in ensuring that minors are not normally able to access services or sections of services dedicated to adult content, and that are effective in ensuring that minors are not normally able to view adult content on other services.

No age verification technique will be 100% effective, but operators should minimize the error rate when minors are mistakenly identified as adults. The harm will be greater if the error is made in the case of a minor in early adolescence and less if the error is made in the case of a minor approaching adulthood.

Reliable age verification may include **document-based** age verification at sign-up and **selfie-based or live likeness** age verification based on video viewing or session. **The use of a document plus a live selfie** at the time of account registration would be considered valid age verification; other methods, such as live selfies and biometrics when accessing content, could also be considered robust, provided they are shown to provide an equivalent level of protection.

I.7 Spanish Data Protection Agency (AEPD) – age verification

The agency has defined a set of principles (https://www.aepd.es/guias/decalogue-principles-age-verification-minors-protection.pdf) that age verification systems must comply with in order to protect minors from inappropriate content. The aim is to ensure the protection of minors, respecting the principles, rights, and obligations set out in the GDPR. The ten principles include the following:

- No user identification and tracking of minors
- No information on the "status" of minors
- Ensuring anonymity
- Verifications applicable only to inappropriate content
- Ensuring the accuracy of checks
- No user profiling during browsing
- No tracking or linking of users' online activities
- Ensuring fundamental rights online
- Define the governance framework

In order to demonstrate that solutions exist that comply with the Decalogue, and that these solutions could be offered via the Internet, the Agency, in collaboration with the General Council of Professional Colleges of Computer Engineering, has developed Proofs of Concept (PoCs) that implement a verification system based on the Decalogue. The results show that a clear separation between identity management, age verification, and content filtering is possible.

Therefore, it has been demonstrated that the identity providers currently implementing the right to personal identity for Spanish and European citizens are already sufficient and that it is not necessary to build parallel digital identity systems to access content that is inappropriate for minors.

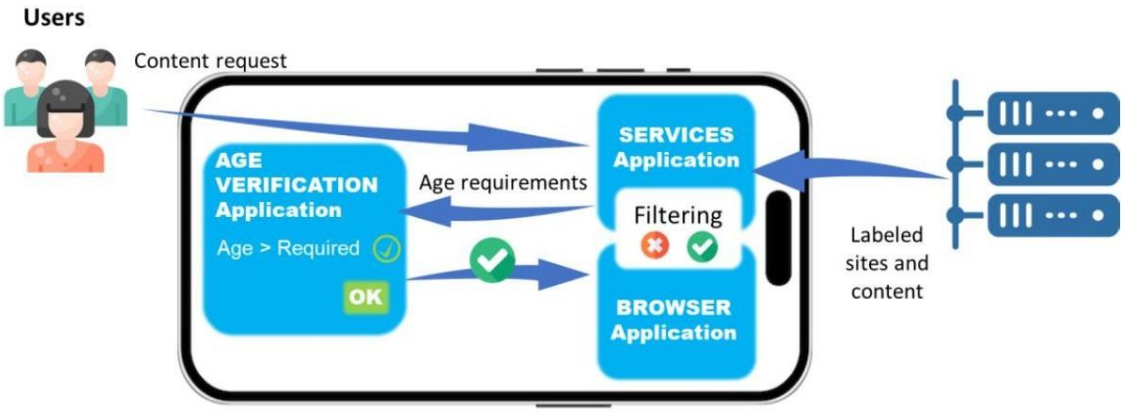
The proofs of concept are also based on the fact that protection against inappropriate content can be carried out on the user's device, with individuals having complete control over their identity and age so that the systems are fully verifiable and transparent.

Finally, the PoCs demonstrate that the location, monitoring, and profiling of minors on the Internet (or Internet users in general) are not necessary to implement protection from inappropriate content.

System description

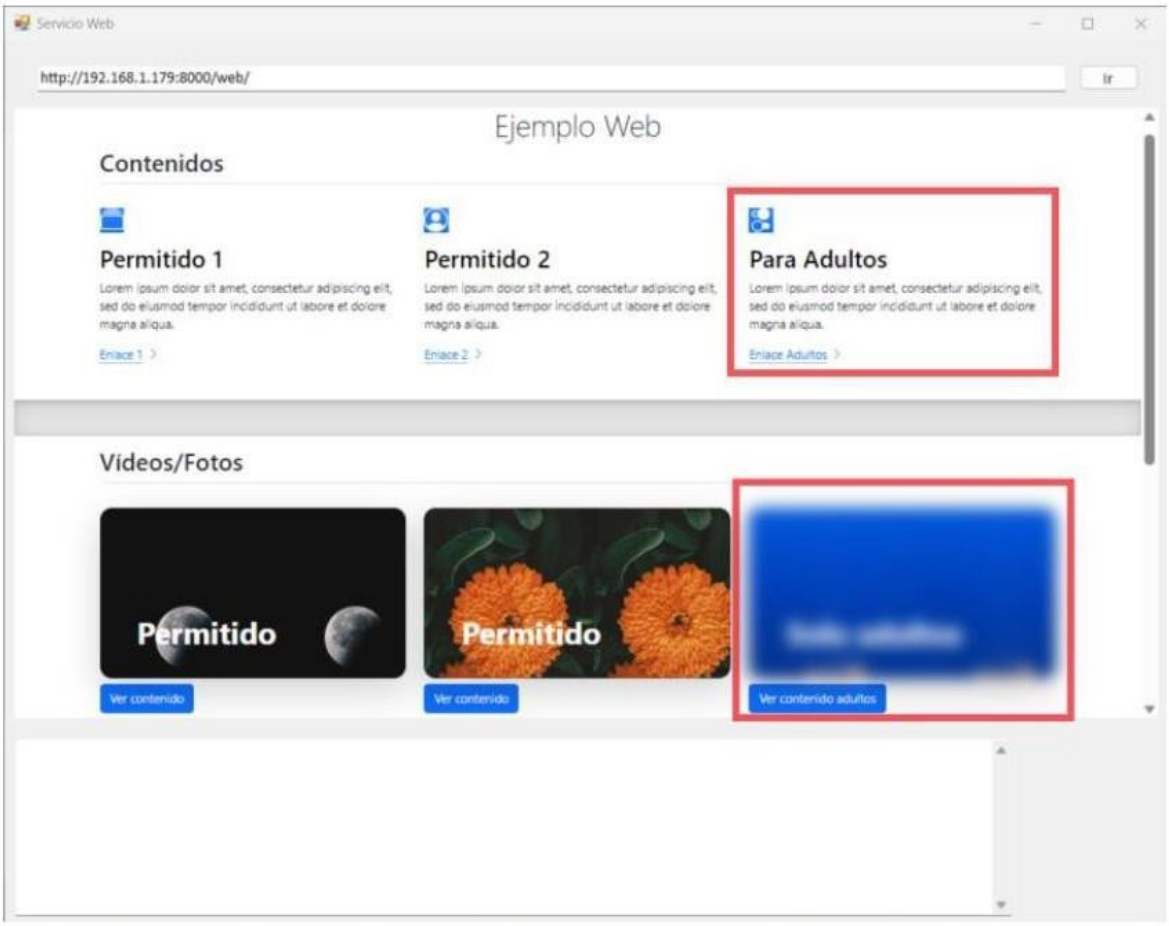
1. All content is classified as "all audience," "for adults," or "inappropriate for minors." In the latter two cases, content is displayed by the internet browser or content app only after age verification.
2. An age verification app is installed on the user's device. The age verification app receives requests as described in point (1), for example via a QR code displayed by the internet browser or directly via the digital wallet installed on the mobile phone. The app verifies the user's age and provides the browser with access authorization.

Below is a summary diagram:



High-level description of the system implemented in the PoCs

The browser masks web content labeled "for adults" or "inappropriate for minors" as shown in the image below. Age verification is required to access this content.

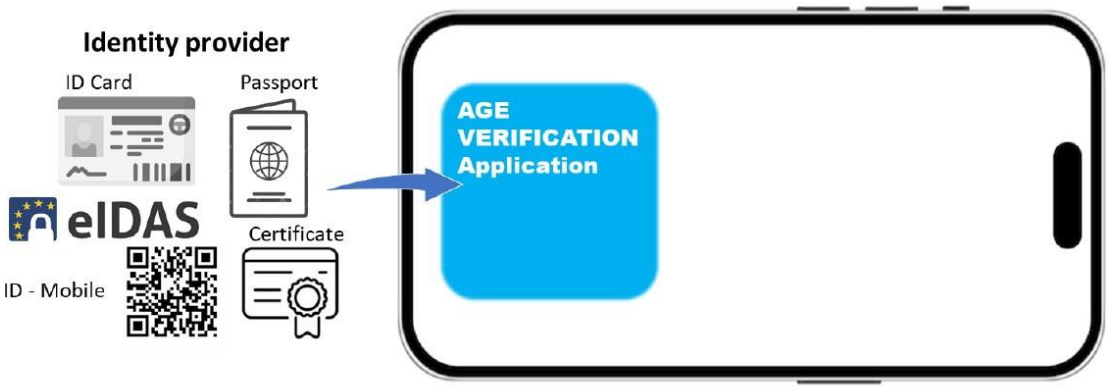


Browser that receives labeled content, but does not display it if it requires age verification

The age verification app acts as an intermediary between different identity providers and the application that needs to verify age in order to allow access to certain content (the browser, for example, or the content provider's app).

The PoCs developed are based on the use of QR codes, digital identities stored in electronic wallets, or physical identity documents. Both processes, registration in an identity management system to use identity and age verification, are considered independent.

The age verification app, which runs only on the personal device and is provided by an entity selected by the user, prevents the dissemination of identity. By placing itself between the identity and the generation of the "authorized to access" condition, this app allows control so that the identity is never revealed to content providers or third parties.

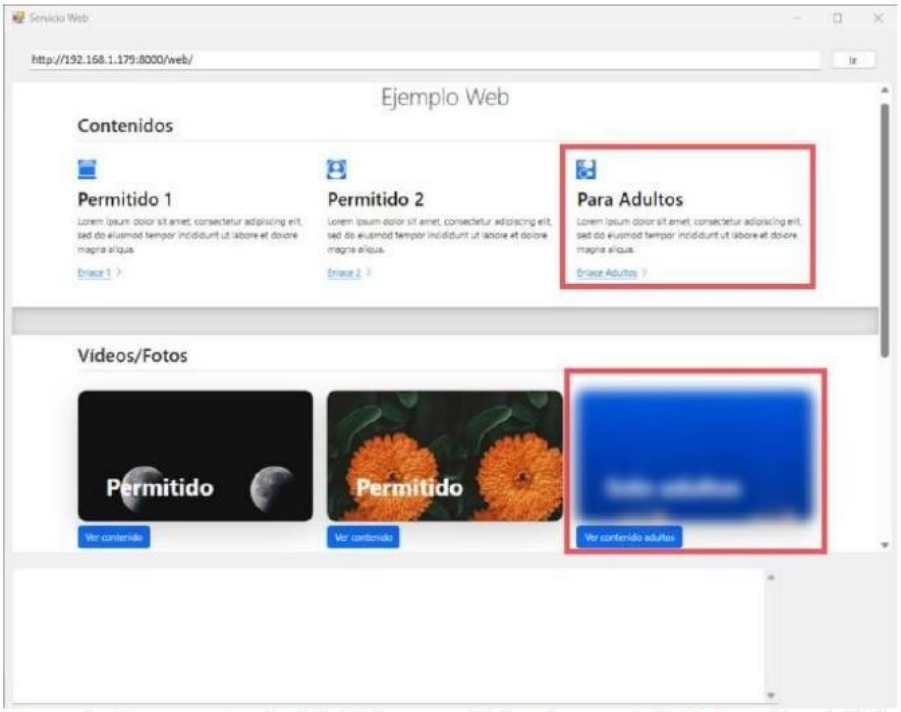


Identity management independent of age verification, which will therefore be anonymous

Example of accessing content from a computer:

1. The user requests access to content labeled "adult" from the browser.

2. The content is received with its label and the display of the content on the device is blocked in advance (in the PoC, the content is shown blurred). In this way, the minor status is not revealed to the content provider, and the content is always served.



Browser che riceve contenuti etichettati, ma non li visualizza se richiede la verifica dell'età

3. The browser calls up the verification application to determine whether the user is of the appropriate age to access the content (over 14, over 18, or other conditions). The age verification application asks the user to show their QR code (on their cell phone) near the camera of the computer or console.

Leggere e controllare il QR nell'applicazione di verifica dell'età

3. Two different situations may occur:

- The age verification application responds with the condition "authorized to access," without revealing any identity information. The browser removes the filter,

  and access to the content is unrestricted.
- The age verification application does not respond with the condition "authorized to access." In fact, it does not respond at all, so after a while the browser stops waiting for a response and maintains the content filter. This may occur because the person is not of the required age (but their status as a minor is not revealed), or because the age verification application has not been installed, or because its use is not authorized, or the QR code is not available, or for any other reason.

Mobile phone use

1. The user requests access to content labeled "for adults" from the browser.

2. The content is received with its label and the display of the content on the device is blocked in advance (in the PoC, the content is shown blurred). In this way, the minor status is not revealed to the content provider, and the content is always served.

Browser che riceve contenuti etichettati, ma non li visualizza se richiede la verifica dell'età

4. The browser calls up the verification application to determine whether the user is of the appropriate age to access the content (over 14, over 18, or other conditions). The age verification application uses the information stored in the digital wallet to perform the necessary checks.

L'app di verifica dell'età riceve la richiesta dal browser e comunica con il portafoglio digitale

The outcome of the verification is the same as in the previous case.

I.8 Observations on the use of public systems

Among the possible solutions to be implemented, without prejudice to the need to preserve the freedom of assessment and choice of technology by regulated entities, in relation to the possible use of digital IDs provided in the public sphere, such as SPID proposed in the opinion of the Garante, the following is noted.

The use of public databases or an authentication system such as SPID could theoretically allow users to prove their age in order to access certain websites or *online* services. However, this system was created to simplify access to public administration services. If its operation required the registration of usage on the servers of state bodies and private companies, **it would have a list of purely private connections and presumed sexual orientations.**

By way of example, the SPID system, for example, does not appear **to be fully compliant with the AGCOM technical specifications indicated below (essentially in the part where so-called double anonymity is required)** for the purposes of implementing the provisions of Article *13-bis* of Law No. 123 of November 13, 2023**.** when the *Service Provider's* authentication request, which contains the domain name of the visited site, is transferred to *the Identity Provider*. In fact, this

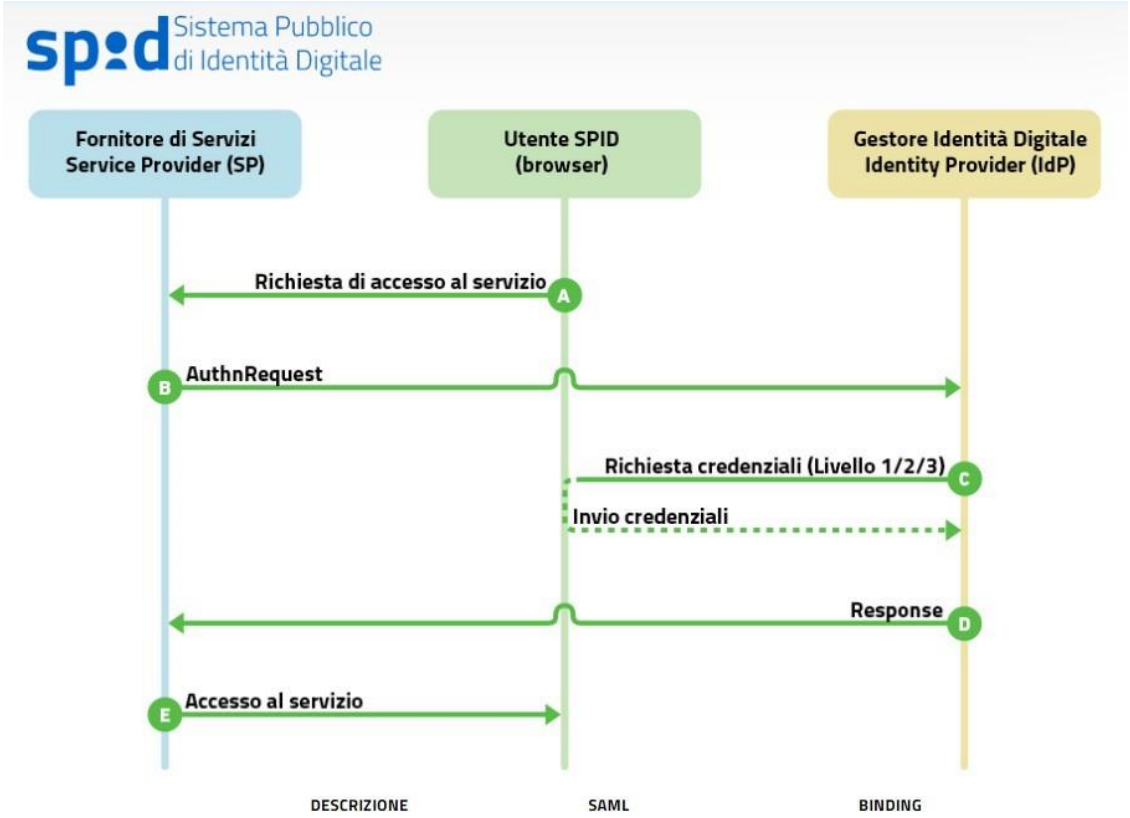
SPID authentication system allows *the Identity Provider* to know the particular site/platform visited by the user, and it cannot be ruled out that this information is stored within the *Identity Provider's* systems.

The *SPID Single Sign On - SP initiated redirect* authentication mode allows the decoupling of *user-service_provider* and *user-identity_provider* interactions. In this way, the *Service_provider* does not communicate directly with *the identity_provider* for authentication purposes, but through the *User_agent.*

As illustrated in the technical documentation for *the SPID Single Sign On* mode [23], messages containing metadata are exchanged from *the service provider* to *the user agent* and *from the identity provider* to *the user agent*.

The authentication mechanism is triggered when the user selects the Identity Manager with which they intend to log in; this selection is made on the Service Provider's website using an official "Log in with SPID" button to be integrated into the service. The Service Provider then prepares an **<AuthnRequest>** to be forwarded to the Identity Manager, where the user is redirected for authentication. Once authentication is complete, the user returns to the Service Provider's website with an assertion signed by the Identity Manager containing the required attributes (e.g., first name, last name, tax ID number) that the Service Provider can use to authorize the user according to its *policies* and provide the requested service.

Below is a diagram representing the flow of the interactions described above.



[23] available at the URL https://docs.italia.it/italia/spid/spid-regole-tecniche/it/stabile/single-sign-on.html#esempio-di-authnrequest

The **<*AuthnRequest*>** message is then sent by *the Service Provider*, via the User Agent, to the Identity Provider's *SingleSignOnService* to initiate the authentication flow. It can be forwarded from a Service Provider *to the Identity Provider* using *HTTP-Redirect binding* or *HTTP-POST binding.*

The documentation published by AGID shows that this **<*AuthnRequest*>** message contains the *"AssertionConsumerServiceURL"* attribute, which indicates the URL of *the Service Provider*, **i.e., the address of the site visited by the user,** to which the response message to the authentication request should be sent (the address must coincide with that of the service reported by the element
<AssertionConsumingService> present in the Service Provider metadata)[24] .

Therefore, this SPID authentication system allows *the Identity Provider* to know the particular site/platform visited by the user, and it cannot be ruled out that this information is stored within the *Identity Provider's* systems.

The following figure shows, in more detail, the flow of messages described in the table.

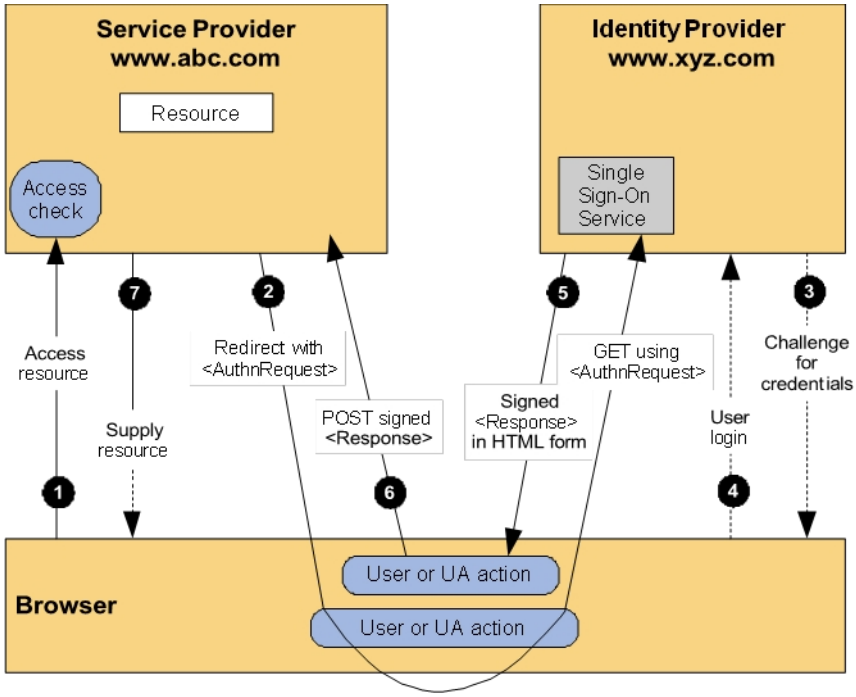


Figura 1 - SSO SP-Initiated Redirect/POST binding

	Description	SAML	Binding
1	The user, using the browser (User Agent), requests access to the resource		
2a	The Service Provider (SP) sends the User Agent (UA) an authentication request to be sent to the Identity Provider (IdP).	AuthnRequest	HTTP Redirect HTTP POST

[24] The response sent by the Identity Provider to the Service Provider can only be transmitted via HTTP-POST binding and must contain, according to these specifications, the Destination attribute, indicating the address (URI reference) of the Service Provider to which the response is sent.

2b	The User Agent forwards the authentication request by contacting the Identity Provider.	AuthnRequest	HTTP Redirect HTTP POST
3	The Identity Provider examines the request received and, if necessary, performs an authentication challenge with the user.	-	HTTP
4	Once authentication has been successfully completed, the Identity Provider performs the user login and prepares the assertion containing the user authentication statement intended for the Service Provider (plus any attribute statements issued by the Identity Provider itself).	-	-
5	The Identity Provider returns the following to the User Agent <Response> SAML containing the assertion prepared in the previous step.	Response	HTTP POST
6	The User Agent forwards the <Response> SAML issued by the Identity Provider to the Service Provider (SP).	Response	HTTP POST

Table 1 - SSO SP-Initiated Redirect/POST binding

It should be noted that step 2b of the above table does not appear to comply with the AGCOM technical specifications (double anonymity), indicated below, when the *Service Provider's* authentication request, which contains the domain name of the visited site, is transferred to *the Identity Provider*.

Therefore, only where the requirements set out in Annex A of the regulation on double anonymity (protection of personal data vis-à-vis the website/platform and lack of knowledge of the website visited/platform by the Identity Provider) are met, does the Authority consider that public systems can be used.

AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

ANNEX C to Resolution No. 96/25/CONS

RESULTS OF THE PUBLIC CONSULTATION REFERRED TO IN RESOLUTION No. 61/24/CONS

1 Summary

I. THE PROCEDURE

With Resolution No. 61/24/CONS of March 6, 2024, the Authority launched the public consultation referred to in Article 1, paragraph 4, of Resolution No. 9/24/CONS aimed at adopting a measure on the technical and procedural methods for verifying the age of majority of users in implementation of Law No. 159 of November 13, 2023.

The following entities participated in the consultation with their own contributions: Meta Ireland (hereinafter referred to as **META**), [**OMISSIS** - a video sharing platform provider], WebGroup

Czech Republic[1] (hereinafter referred to as **WEBGROUP**), Aylo holdings[2] (hereinafter referred to **as AYLO**), [**OMISSIS** - an electronic communications operator (hereinafter referred to as **an operator**)] , the Italian Data Protection Authority for Children and Adolescents (hereinafter referred to as **GARANTE PER L'INFANZIA)**, the National Council of Users (hereinafter referred to as **CNU)**, Italian Parents Movement (hereinafter referred to as **MOIGE)**, Altroconsumo, Forum of Family Associations (hereinafter referred to as **FAF)**, Italian Women's Center (hereinafter referred to **as CIF)**, Christian Workers Movement (hereinafter referred to **as MCL)**, Noi Trento APS (hereinafter referred to as **NOI TRENTO)**.

Following receipt of the written contributions, hearings were held with the participants in the proceedings in May 2024.

The results of the public consultation are outlined below.

II. GENERAL CONSIDERATIONS

A. Comments from institutional entities, operators, and associations

On the need for effective age verification systems

The **CHILDREN'S OMBUDSMAN** states that the constant and rapid evolution of the digital world and the development of new and increasingly engaging ways of interacting with the various devices and software that are part of it make it increasingly urgent to implement an effective system of regulation and protection from the risks that may arise, especially for the most vulnerable individuals. This need is made all the more pressing by the growing and widespread use of artificial intelligence, which is leading to further transformations with unpredictable outcomes. It considers that, although appreciable progress has been made in introducing various tools and mechanisms to protect young users from the dangers of the internet, many of these measures are still wholly insufficient. It adds that it is clear that most age verification systems are still based on methods that are easily circumvented, which leads to a clear and significant vulnerability of minors, as they are potentially exposed to content and services that are very harmful to their physical and mental health. While recognizing that the problem is very complex and difficult to solve, also due to the lack of standardization and consistent regulation

[1] WebGroup Czech Republic, a.s. is a company incorporated in the Czech Republic that operates the XVideos website available at www.xvideos.com. XVideos hosts and makes adult videos available to users free of charge. Users can also create an account to upload their own content online and receive compensation in return. XVideos is a business model based on Internet traffic and advertising and does not involve the sale of adult content.

[2] Aylo Holding S.à.r.l. is a technology and media company that owns a broad portfolio of adult entertainment businesses (Pornhub, YouPorn, Redtube, Brazzers). Its main activities consist of free and subscription-based video streaming sites. Aylo's main business units are as follows: video sharing platforms (VSPs), paid sites, content platforms for models, advertising platforms, and video game platforms. ([3]) Filtering software generally refers to software installed on a device that can filter adult web pages/content (at the web browser level, as proposed by Spain, or even at the parental control application software level)..

in different countries, which can create disparities and gaps in protection systems, making it impractical to adopt truly effective solutions on a global scale, the GARANTE appreciates that the Authority has implemented a regulation that the legislator has given urgent priority to and which aims to introduce an age verification system capable of preventing minors from accessing websites and platforms for sharing pornographic images and videos.

The **CNU** appreciates Agcom's focus on protecting the rights and legitimate needs of minors as active participants in the communication process, as also provided for in the Convention on the Rights of the Child, and believes that the launch of the public consultation on how website operators and video sharing platform providers can verify the age of users will help prevent minors from being exposed to content that is inappropriate for their age content that could undermine their psychological and physical well-being. **It therefore states that the solution put forward for consultation by the Authority, with the favorable opinion of the Privacy Guarantor, has the full support of the CNU.** It also believes that it is necessary to define age verification methods so that they are clear, effective, and verifiable through a robust certification and interoperability framework, as the online age verification methods already available on the global market often pose risks to privacy and cybersecurity because they involve excessive processing of personal data, such as ID card data, credit card data, facial recognition, or even analysis of the user's online behavior. These methods require excessive proliferation of sensitive data that is beyond the control of the data subjects and poses risks in terms of security and transparency. Other verification methods (such as self-declaration) are very ineffective as they can be easily circumvented, while others are characterized by a high margin of statistical error. In such cases, there is a risk that minors will be able to access harmful and inappropriate content without restrictions or controls.

MOIGE emphasizes, in pursuit of the best interests of minors and in order to guarantee them maximum protection online, the legal relevance of the issue of minors' access to social networking platforms and all information society services, considering that the use of such services is still a contractual activity as it is subject to the conclusion of a contract and the related conditions of use of the services offered by providers. It therefore notes a contradiction within the legal system, as the legislation allows minors over the age of fourteen to use electronic communication services, although in order to access social networking platforms it is necessary to sign actual contractual clauses, accept the terms of service, and give consent to the processing of personal data for the purposes inherent in the execution of the contract. In fact, in order to access social networking sites, it is necessary to sign the conditions of use, which are actual contractual clauses, accept the terms of service, and give consent to the processing of personal data for purposes related to the execution of the contract. He points out that, under Italian law, minors cannot legally dispose of their rights and interests, e.g., property rights, since the law attributes the capacity to act to those who have reached the age of majority. However, it adds that, due to a sort of communicating vessels phenomenon, the subjective condition for consenting to the processing of personal data under EU Regulation 2016/679 has become

in fact, not in law, a sufficient requirement for the conclusion of a contract for the provision of services, without any consent from the person exercising parental responsibility. Therefore, it considers that the appropriation of minors' personal data by means of the artifice of differentiating the age for accessing information society services from the age for performing any other legal activity is unlawful and in violation of mandatory rules of Italian law and of any legal system that requires the age of 18 to be reached in order to acquire legal capacity. Due to a sort of communicating vessels phenomenon, the subjective condition for giving consent to the processing of personal data pursuant to Article 6(1)(a) of Regulation (EU) 2016/679 has become, in fact, even if not by law, a subjective condition for the conclusion of a service provision contract, given that the possibilities for effective control over the age of the contractor-user are limited, unless effective measures are urgently applied to verify the age of users of sites and services that display content or activities unsuitable for minors. Furthermore, it emphasizes that, pursuant to Article 17 of Legislative Decree 70/2003, information society service providers are not required to monitor the information they transmit or store, so that civil liability for acts committed by minors on the internet falls on those exercising parental responsibility: for this reason, it is necessary and urgent that parents be given back the real possibility of control and decision-making over their minor children's use of social networking platforms and that the age of eighteen be restored as the minimum age for validly expressing any type of will and consent, including for the provision of information society services. Finally, it requires the adoption of systems that, with maximum effectiveness and security, guarantee a specific expression of consent by those exercising parental responsibility for access to platforms that provide communication services or make audio and video content available.

NOITRENTO supports the need for real *age verification* for accessing websites that require users to be of legal age.

The **MCL** argues that the online age verification methods used to date have not been able to protect minors from content that can harm and compromise their physical, mental, and moral development and well-being. psychological, and moral development. It therefore considers it urgent to identify and implement new mechanisms that guarantee a high level of protection and, while respecting privacy, prevent minors from accessing content and activities that irreparably damage their harmonious and integral development. It also requests that this public consultation not be a one-off initiative, but rather that it activate a constantly monitored and updated protection system capable of involving and supporting families.

The **CIF** confirms its full approval of the measure governing the technical and procedural methods for verifying the age of users.

ALTROCONSUMO considers it useful to add the definitions of 'proof of age' and 'certifying entity'. It points out that the principle of proportionality must act as a counterbalance in weighing up the rights and freedoms to be safeguarded, such as freedom of expression and the right to privacy, and that verification systems must operate with an excess of guarantee, as it is better to protect

an adult 'erroneously' than to fail to protect a minor. For such cases, it proposes providing for *ex post* 'correction' systems in the event that an adult is blocked from using a website or content.

The **FAF** welcomes the opening of the public consultation on the technical and procedural methods that the subjects identified by the regulation are required to adopt to verify the age of users, but believes that action is needed on several fronts. In fact, in addition to the parental control filter set up by operators, it believes that sites that distribute video material intended for an adult audience, such as Pornhub and many others like it, should also set up adequate forms of age verification.

On the need for a harmonized approach at European level

META, while understanding that the aim of the law is to prevent access to pornographic content (and therefore not directly applicable to Meta), believes that access to inappropriate content or content intended for adult audiences should be considered within a broader and more structured framework; rather than focusing on the introduction of various *age assurance* methods adopted by different entities, which, in addition to creating a fragmented and ineffective framework, could pose significant risks in terms of data minimization. Furthermore, in order to ensure their effectiveness, it considers it necessary for these solutions to be discussed at the European level, as well as at the industry level. Similarly, it considers it essential that all apps are subject to the same standards in order to ensure a consistent and effective approach to the protection of young people. Collaboration across the entire sector on this issue would ensure safe and age-appropriate experiences, while also preventing young people from migrating to apps that are less secure than those that have invested in security and age-appropriate experiences. Finally, it believes that a multi-level approach to age verification should be adopted, allowing users to choose an *age assurance* mechanism based on feasibility and preferences, so as to ensure fairness and objectivity in the process.

B. **Assessments by the Authority**

The Authority acknowledges that both institutional entities and private individuals are aware of the need for an effective age verification system and that the solution proposed by the Authority is suitable for balancing the requirements of effectiveness and personal data protection. It also agrees that the issue of access to inappropriate content or content intended for an adult audience should be considered in an international or, at least, European context in order to avoid a fragmented framework and ensure the effectiveness of solutions. It also agrees on the need for all apps to be subject to the same minimum standards in order to ensure a consistent and effective approach to the protection of young people. The Authority therefore adopts a *future-proof* approach with these technical specifications, which both complies with the requirements of Decree-Law 123/2023 (as converted into law) and is capable of incorporating and complying with future EU provisions on age verification systems and the decisions that will be taken in this area.

III. OBLIGATIONS AND SUBJECTIVE AND OBJECTIVE SCOPE OF THE GUIDELINES

A. Comments from institutional entities, operators, and associations

The **CHILDREN'S OMBUDSMAN** hopes that **this protection** can **be extended to other content that is seriously harmful** to the physical and mental health of children and adolescents, such as content that incites hatred, violence, and other improper and harmful practices, even if not included in the scope of the consultation.

ALTROCONSUMO believes that the **guarantee systems outlined above can be applied to content subject to *parental control* as referred to in Resolution 9/23/CONS**, including, but not limited to: adult content, gambling, betting, content relating to weapons, drugs, violence, hatred, and discrimination, the promotion of practices that may be harmful to health in light of established medical knowledge, and sects.

META recommends limiting the definitions contained in the text to only those subjects defined in Article 13 bis of Decree-Law No. 123 of September 15, 2023. In particular, it considers that **the definitions of "regulated service" and "regulated entity" should only include services and entities that facilitate access to pornographic content,** as defined in Article 13 bis of Decree-Law No. 123 of September 15, 2023, No. 123, avoiding a generalized application to other types of services that offer content reserved for adult users.

AYLO believes that the definitions **should cover not only video-sharing platforms, but all websites and social media that are even capable of sharing sexually explicit content**. In fact, it points out that if age verification systems were implemented only on specific platforms that disseminate sexually explicit content, as has been the case in other jurisdictions, almost no users (regardless of age) would continue to visit such sites and users would simply move on to other, numerous sites without age verification and estimation systems, which would probably be less compliant with the law and subject to significantly lower reliability, security, and content moderation measures. Therefore, it believes that the effective protection of minors would be null and void, as users would simply move to less protected and non-compliant sites. Furthermore, it points out that users who decide not to move to other sites would use other methods to circumvent age protection requirements, whatever form they may take. On this issue, AYLO states that there are hundreds of thousands of sites classified as adult sites and that the largest and most visited adult content websites are, in fact, the ones most likely to comply with the law, as they are able to invest more resources in reliability, security, and moderation processes, thus limiting the availability and potential exposure of visitors to illegal, obscene, or harmful material. Therefore, while the most responsible website operators will be able to comply with this legislation, others will not (and have not done so to date in countries where regulation has been introduced), leading to a substantial increase in the risk of users being exposed to potentially harmful material.

harmful on websites without adequate controls. For example, in US states where AYLO introduced age verification and age estimation or removed access to its platforms, there was a surge in searches for other adult sites, often unregulated, with reduced or non-existent reliability, security, or moderation processes, as well as searches for virtual private networks (VPNs).

In particular, AYLO presented the case of the state of Louisiana (US) where, in 2023, following the adoption of a law requiring websites/platforms providing pornographic content to verify age via electronic ID cards, there was an 80% decrease in access to its platform and, at the same time, an increase in searches for alternative sites, methods of circumventing controls, and use of VPNs.

In light of the above, it considers it essential that, in order to protect minors from adult content online in the most comprehensive and effective way, the scope of these obligations should be sufficiently broad to include all content of this type.

In conclusion, AYLO believes that in order to ensure that minors are protected from adult content online, the scope of the new legislation should be broad enough to include all potentially harmful content, including social media websites that allow the viewing of adult material, emphasizing that a device-level solution would be the best option for blocking other content that is unsuitable for minors.

WEBGROUP believes that if a broad requirement is introduced establishing *age verification* mechanisms for all audiovisual content on VSPs deemed harmful, **such requirements should comply with European Union law and, in particular, with the law of the country of origin,** as enshrined in Directive 2000/31/EC of the European Parliament and of the Council of June 8, 2000, on certain legal aspects of information society services, such as electronic commerce, in the internal market (Directive on electronic commerce). Those requirements should also comply with the principle of proportionality in terms of using the least restrictive means possible to achieve public policy objectives and should ensure an appropriate balance between the protection of minors and the fundamental rights at stake.

[OMISSIS - A video sharing platform provider] believes that the **rule would not apply to [OMISSIS - A video sharing platform provider]** as **a provider established in a third country** and because the company does not allow users to distribute pornographic content via its platforms; however, it agrees with the need to establish mechanisms to protect minors from adult content. It adds that the **development of a European *age assurance* framework is the right way forward and**, therefore, such efforts should also be taken into account for the purposes of the measure under consultation.

[OMISSIS - A video sharing platform provider] believes that, in order to adequately protect minors online, *age assurance* tools must be: (i) proportionate; (ii) respectful of users' personal data protection rights and *user experience*; and (iii) simple and effective. It agrees with the Authority that it is essential that any initiative taken in this area be proportionate. It follows that *age assurance* measures should restrict minors' access to content without infringing on their personal data and fundamental rights by

excessively restrictive protection tools. In this context, it is also worth noting that **Article 28 of the DSA requires online platforms to take "appropriate and proportionate" measures to ensure the protection of minors online, but does not impose any obligation to adopt *age assurance* tools, the adoption of which remains at the discretion of providers.** In fact, *age assurance* is only one of the solutions available for the protection of minors online and can be designed in different ways, depending on the specific characteristics of the service in question. In this regard, pursuant **to Article 35(1)(j) of the DSA, *age assurance* could be considered a potential risk mitigation measure for Very Large Online Platforms (VLOPs), also with reference to the risks identified in Article 34 of the DSA (which also includes risks to minors).**

[OMISSIS – An operator] argues that the obligations and responsibilities for implementing *age verification* procedures should apply exclusively to the categories of entities identified by the legislation, and not to entities that do not offer video sharing content or platforms, such as **electronic communications service providers. It considers that the latter, having no connection with such services, should be considered outside the category of regulated entities for the purposes of this consultation.**

At the same time, it considers that electronic communications operators should not be obliged to provide this service and therefore to process age verification requests. With a view to not shifting an obligation incumbent on websites and platforms onto independent third parties, it considers that **operators should retain discretion in providing this *age verification* service to regulated entities**. In fact, it does not consider it proportionate to require operators to comply with every age verification request from websites on a mandatory basis. It points out that the exceptional number of requests that the entity responsible for technically performing the verification activity would have to process and the investments that would be necessary, particularly in view of a possible expansion of the scope of application of the proposed regulation, cannot be ignored.

B. Assessments by the Authority

The Authority notes that the GARANTE PER L'INFANZIA (Italian Children's Ombudsman) hopes that the age verification system proposed for the protection of minors can also be extended to other content that is seriously harmful to the physical and mental health of children and adolescents, such as content that incites hatred, violence, and other improper and harmful practices, even if not included in the scope of the consultation. ALTROCONSUMO shares this view and believes that the guarantee systems outlined could be applied to content subject to *parental control* as referred to in Resolution 9/23/CONS. On the other hand, META and AYLO believe that **the definitions of 'regulated service' and 'regulated entity' should only include services and entities that facilitate access to pornographic content. WEBGROUP** believes that if a broad requirement is introduced establishing *age verification* mechanisms for all audiovisual content of VSPs deemed harmful, **such requirements should comply with European Union law a n d , in particular, with the law of the country of origin.** Also [**OMISSIS - Un**

video sharing platform provider] believes that the **rule would not apply to it** as **a provider established in a third country** and that the **development of a European *age assurance* framework is the right way forward; where appropriate, in line with Article 35(1)(j) of the DSA, *age assurance* could be considered a potential risk mitigation measure for Very Large Online Platforms (VLOPs), also with reference to the risks identified in Article 34 of the DSA (which also includes risks to minors).**

With reference to the comments made by META, AYLO, and WEBGROUP regarding the existence of the obligation and the subjective scope of application, the Authority, also considering the proposals made by the GARANTE PER L'INFANZIA (Italian Data Protection Authority for Children) and the consumer association, deems it appropriate to clarify, in view of the comments made by some of the parties involved in the public consultation, that the rules governing the technical and procedural methods for verifying the age of users, which are approved by this resolution in implementation of Article 13-bis of Decree-law no. 123/2023, converted, with amendments, by law no. 159/2023, must be adopted by website operators and video sharing platform providers that disseminate pornographic images and videos in Italy, wherever they are established.

On this point, the Authority considers that, in light of the regulatory context referred to above and the comments made by participants, the technical and procedural methods for verifying the age of users approved by this measure are highly recommended, as they are effective, appropriate, proportionate, and functional, for their use by parties other than those directly regulated herein and with reference to additional types of content, beyond pornographic content, that could nonetheless be harmful to the physical, mental, or moral development of minors, such as the categories provided for in Resolution 9/03/CONS.

In agreeing with AYLO's observation, the Authority considers it reasonable that the objective scope of application should cover not only video-sharing platforms, but all websites and social media that are capable of sharing sexually explicit content. With regard to the observation that only large website and platform providers are likely to implement the measures in question, it is considered that adequate supervision, including through the cooperation system provided for in *the Digital Services Act,* and adequate regulatory safeguards will act as a deterrent. Furthermore, under the TUSMA, as clarified below, the Authority may in any case prohibit the circulation of harmful content disseminated by providers established in other countries to users located in Italy.

With reference to the observation of **[OMISSIS - An operator],** the Authority considers it reasonable, where private individuals intervene as third parties, that the owners of video sharing platforms and websites interact with the latter through agreements resulting from commercial negotiations.

IV. METHODS OF IMPLEMENTING AGE ASSURANCE SYSTEMS

A. Comments from institutional entities, operators, and associations

The **CHILDREN'S OMBUDSMAN** believes that, among the various solutions proposed in the consultation, in accordance with what has already been proposed within the Technical Committee on the protection of children's rights online in the context of social networks, digital services and products established at the Ministry of Justice by Ministerial Decree of June 21, 2021, **the adoption of a system based on the use of a SPID-type digital identity allows for a high degree of certainty** in determining the age of the user and, at the same time, in compliance with the principle of proportionality, offers the necessary guarantees of personal data protection and protection from content harmful to minors. This is in line with the European Commission's call in its new European strategy for a better internet for children (BIK+), adopted on May 11, 2022, which invited Member States to support effective age verification tools in line with the recently adopted European legislation on digital identity (EU Regulation of March 26, 2024). Furthermore, while recognizing that other solutions make it easier to achieve reasonable levels of protection, it considers that the protection of minors cannot be limited to the use of systems already used in the past, such as parental control, a tool which, although very flexible and adequate for protecting minors online when activated, has not been widely adopted in either traditional or new media due to its limited use by adults, often because of certain difficulties in its use.

WEBGROUP emphasizes the importance of considering that *age verification* can be carried out more efficiently at the user's device level, for example in the form of filtering software (APP), rather than at the website level. This gives users complete control over their identity and age and minimizes the amount of data shared with pornographic websites that would remain on the device. In support of this, it states that the **Australian government** recently decided, after passing a law favoring *age verification*, to no longer implement *age verification* due to a detailed study that confirmed numerous problems with the technology involved. Specifically, the Australian government is currently working with industry representatives to develop effective educational mechanisms for parents to **use device-level filtering software to restrict children's access to harmful material.**

As a further example, he adds that **Spain has** also **recently launched a pilot program, developed by the National Data Protection Agency (DPA), which plans to carry out *age verification* at the device level**.

The solution envisaged by the Spanish DPA is based **on content labeling** (using *tags*) by online service providers, which allows content to be classified as sexual, violent, and/or racist. Access restriction is performed locally on the user's device rather than by the online service provider or even by third parties such as intermediaries. The system is based on a virtual interaction between the PC *browser* and an app installed on the user's cell phone. In this way, access to adult content via the PC *browser* is managed by an age verification app that must be installed on the user's cell phone. The PC browser, analyzing the *tags* related to web content, will ask the user to verify their age—by scanning a QR code presented by the browser itself with their mobile phone—to the app installed on the mobile phone to grant or deny access to specific content previously labeled by online sites and platforms as adult or inappropriate content. On the other hand, when it comes to accessing content directly from a cell phone, eWallet solutions compatible with the eIDAS regulation are used, which work on "age attribution" systems to provide confirmation of a specific age, respecting the principle of data minimization. In this case, the mobile browser will request verification and interact with the eWallet app, also on the mobile phone, which provides the attribute of legal age.

WEBGROUP believes that **the solution provided for by the Spanish DPA is appropriate for balancing the objectives of *age verification* systems** (i.e., preventing minors from accessing adult content) and the protection of adult users' rights, which include constitutionally protected rights such as freedom of expression and the right to privacy, as well as user safety and national security. Furthermore, it notes that minors are generally more at risk of being exposed to adult content from social media websites and search engines than from traditional adult websites such as XVideos. It believes that search engines allow anyone to access a large amount of adult images and videos (content that is no less explicit than that found on XVideos) in a matter of seconds. For example, the association explains that Facebook reported as many as 73.3 million explicit posts as "child nudity and sexual exploitation" in the first nine months of 2022 alone, and the same is true for other popular sites such as YouTube, Twitter (now X), TikTok, Reddit, Snapchat, and LinkedIn, not to mention much less popular but easily accessible websites. Finally, it reiterates that filtering software, or **device-level filtering software[3] can be more effective in preventing minors from accessing explicit content online and a wide range of adult content.**

WEBGROUP believes that if the ***age verification*** **procedure is performed at the device level using filtering *software***, without the intervention of third parties, the risk of third-party independence is eliminated. Furthermore, it believes that the introduction of a third party as a repository for any information inevitably adds an additional layer of concern for the protection of such data. *Age verification* performed on the device adequately balances the interests of minors with the other rights of all Internet users, such as user anonymity. In this regard, it believes that **what is currently implemented by digital identity providers (such as the government authority that issues an electronic ID card or certificate) is sufficient,** and not

[3] Filtering software generally refers to software installed on a device that can filter adult web pages/content (at the web browser level, as proposed by Spain, or even at the parental control application software level).

It is necessary to create an alternative digital identity system for *age verification* purposes before minors access adult content.

WEBGROUP believes that a **device-level *age verification*** system would ensure that systems are fully verifiable and transparent, especially in light of the high risks posed by some existing *age verification* tools. In this regard, it points out that some of the most widely used *age verification* systems are developed by third parties, rather than by the website itself, and that *age verification* carried out by content providers, rather than by individuals on their devices, jeopardizes their rights and freedoms and is not effective in preventing minors from accessing adult content, putting the privacy of website visitors at risk (e.g., when identification information provided for age verification is disclosed by hackers or others). Furthermore, it believes there is a risk that the entity performing *age verification* may locate minors or collect their data. It believes that *age verification* poses a risk of blackmail for national security when access data is compromised. It adds that *age verification* imposed on platforms is highly ineffective in the face of a range of inexpensive and easily accessible technologies, such as virtual private networks (VPNs), and ineffective in geolocating individuals, with the result (especially near national borders) that individuals are not subject to age verification because the *age verification* provider mistakenly believes that they are outside the region subject to the requirements and vice versa. **It believes that age should be verified on the personal device via an app chosen by the user,** avoiding the transmission or sharing of personal identity data. This app, interposed between the identity and the generation of the authorized user status, allows age to be verified without imposing verification on platforms, with the advantage of avoiding all the risks that AV imposed on platforms entails. Alternatively, WEBGROUP believes that each provider should be free to choose the *age verification* mechanisms deemed appropriate, and users should be free to choose the most convenient of the systems offered, subject in both cases to the principles of effectiveness and compliance with the law. It believes that the Authority **should provide a list of controlled/certified AV service providers.**

WEBGROUP also believes that, from a proportionality perspective, it is reasonable **to make parents and guardians aware, first and foremost, that the most widely used computer operating systems, Microsoft and Apple, include parental control features by default at no additional cost.** It adds that all major browsers, including Google Chrome, Mozilla Firefox, Microsoft Edge, and Apple's Safari, also have parental control options, and if parents wish to add additional parental control features, they can easily purchase additional software such as Bark or NetNanny, or even download additional free software such as Questodio, Kaspersky Safe Kids, FamilyKeeper, and others. These features allow parents to block access to sexually explicit material on the web, prevent children from giving personal information to strangers via email or in chat rooms, limit children's viewing time, and keep a log of all online activity on a home computer. He adds that parents can also use screening software that blocks messages containing certain words, as well as tracking and monitoring software, and that they can also limit and observe a child's Internet use by simply placing a computer in a public space within the home. All of these methods are inexpensive (or

free) and non-intrusive (from the point of view of the principle of proportionality) ways to achieve effective *age verification*.

WEBGROUP believes that, given the current state of technology, **facial recognition may not be technically secure or adequate**, as there is a wide margin of error with regard to age and, furthermore, the collection of biometric data also poses serious risks to the privacy of Internet users.

WEBGROUP also considers it necessary to add definitions of "parental control," "filtering," and "device-level age verification."

AYLO believes that **the real solution to protecting minors and adults is to verify the age of users at the point of access—i.e.,**[on] **users' devices—at the operating system level** and to deny or allow access to age-restricted materials and websites based on that verification. This approach requires the **cooperation of operating system manufacturers and**, with their consent, would minimize the transmission of personal data while protecting minors from harmful content. This would ensure greater ease of implementation, as there are far fewer operating system manufacturers than websites/platforms providing pornographic content. In addition, there would be greater protection of personal data, which would not be managed by a multitude of websites, and greater effectiveness of protection would be ensured, as minors would be blocked from accessing any pornographic content, including illegal or 'extreme' content, regardless of whether websites/platforms implement protective measures. This solution could be implemented by ensuring that **operating system manufacturers block adult content by default,** so that minors are always protected when accessing the Internet, and **require age verification at the device level only when the user requests access to adult content.**

AYLO points out that when age verification and estimation are performed on the device, users perform this verification only once, through the operating system, and not on every website subject to age restrictions. This drastically reduces the risks of data theft and privacy breaches and creates a process that is very easy for regulators to monitor. In **AYLO's** view**,** the technology to achieve this already exists today, as many devices already offer **free and** easy-to-use **parental control features** that can prevent minors' accounts from accessing adult content without risking the disclosure of sensitive user data. It adds that these features simply need to be improved to ensure adequate age verification or estimation and then be able to block devices by default, unless they are unlocked after age verification or estimation by an adult on the device. Finally, it believes that solutions implemented at the device level

[4]For device-based age verification, AYLO means any approach to age verification and estimation where personal information used to verify the user's age is shared in person at an authorized retailer, entered locally on the user's device, or stored on a network controlled by the device manufacturer or device operating system provider. Through pre-installed content blocking and filtering software, the disabling of web browsing permissions, or other means, the user cannot access age-restricted content on the internet unless they have been verified as being of age or older. To be implemented, this approach requires the cooperation of developers and operating system providers.

These would be the most effective in terms of functionality, ease of use, and lack of barriers to use, as they would remain confined to the device environment, which is chosen and set up according to the user's needs, and moreover in a well-known digital environment.

AYLO argues that, although an approach of implementing age verification at the website/platform level may work for structured and ethically oriented companies such as AYLO itself, this could lead to a risky situation where sites that do not adhere to ethical standards or have little experience in the field would implement ineffective or unsafe age verification and age estimation systems that are easily circumvented or capable of collecting users' personal data. In general, **it does not believe that website-level age verification and estimation methods are effective.** It argues that, as demonstrated by other jurisdictions that have implemented website-level solutions, these have proven ineffective as minors are still able to easily and readily access adult material online, because compliance with such requirements is met by only one or a few adult platforms and their implementation is poor. In light of the above, **it believes that the only effective solution to prevent minors from accessing adult content is device-level age verification through the operating system,** where the default setting for all accounts and all devices on the operating system is to block adult content.

AYLO argues that it is difficult to consider any *age assurance* mechanism implemented at the website/platform level to be proportionate, with the exception of the self-declaration method. It believes that *age assurance* systems at website level other than self-declarations are not proportionate measures in light of the amount of risk they create and the damage they cause both to the users concerned and to the commercial livelihood of video-sharing platform providers. In this context, it points out that, in the case of age verification implemented at website level, there is a risk that anyone, including minors, will be driven to non-compliant sites (i.e., those that decide not to implement such verification), and it is very likely that users, including minors, will thus be exposed to illegal and "extreme" content with which they would otherwise never have come into contact. Therefore, the negative social consequences of adopting such a tool would be significant and wholly unacceptable, **even though they could be entirely avoided through the implementation of device-level controls. It considers that age verification and age estimation systems implemented at website level are always disproportionate,** insofar as the ultimate objective is to prevent risks to minors. Furthermore, it argues that age verification and estimation systems at website level are also disproportionate in view of the economic rights and freedoms of platforms. In fact, it considers that any requirement to implement identity certification on their platforms would inevitably lead to an almost total loss of visitors to the platforms themselves, who would simply move on to other activities, and, as a result, the very existence of the platforms would be put at risk, as they would have almost no chance of surviving the total loss of traffic on them.

META believes that a significant step forward can be taken at European level to ensure that parents only have to verify their child's age once and that minors have

subsequently access an age-appropriate experience in each individual app. **It believes that**, instead of forcing parents to track down the numerous existing applications and all those that will be developed in the coming years, **age verification should be carried out directly in the (virtual) place where teenagers download the application itself (app store or operating system level).** According to the operator, this approach would reduce the burden on parents of identifying the multiple apps used by their children and juggling different age verification systems, minimizing the number of times and (virtual) spaces in which potentially sensitive data must be shared to verify age. Furthermore, parents and teenagers would not be forced to provide their identity documents to all apps in circulation to verify their age or that of their children. Moreover, it points out that teens and parents already provide ***app store*** **operators** with this information when purchasing devices and creating accounts, and that *app stores* have already integrated notification, review, and approval systems that could be used directly by parents. **It therefore believes that verifying a teenager's age at the *app store* level would ensure that apps downloaded from the app store must meet the same protection standards and provide content and experiences appropriate to the age verified.** At the same time, it would also promote a healthier and more competitive market, as **the requirement to verify age at the time of registration for each individual app** would create a significant barrier to entry and an insurmountable obstacle to the development of new players in the market. Finally, it believes that facilitating age verification for new apps targeting teenagers would not only promote competition, but also provide parents with greater assurance that all apps, even those they have never heard of, comply with regulatory requirements.

[OMISSIS – An operator] believes that a network operator has sufficient information to carry out an effective *age verification* process only under certain conditions, as in most cases it would have no way of determining with certainty whether the user (i.e., the actual user) is an adult or a minor. Furthermore, they cannot be held liable in any way if the adult does not take action to protect the minor from accessing sensitive content or if a minor actively decides to circumvent the security mechanisms put in place to protect them. One solution could be to verify age using contractual information associated with the IP address used by the user. This solution would allow the IP address used by the user while browsing to be linked to the contractual information of the SIM card holder available to the Operator. Verification via IP address requires a necessary distinction between the user's browsing via a mobile network or a fixed network. In the case of mobile network browsing, it would be possible to compare the user's dynamic IP address with the contractual information available to the Operator only for a subgroup of users who require proof of age from the mobile network. In fact, **for the purposes of *age verification,* the Operator would only be able to determine with certainty whether the user is a minor in the case of a user who uses a 'Junior' SIM card registered to the minor themselves.** In this case, [**OMISSIS - An operator]** explains that the dynamic IP used by the Junior user (holder of a "Junior SIM") to browse the mobile network would be associated by the Operator with the SIM of a minor, resulting in a KO on the age verification. Conversely, if the dynamic IP address is associated with a SIM card registered to an adult (e.g., in the case of a father who registers

the SIM card and allows their minor child to use it, or in the case of an adult user), the Operator would approve **the age verification based on the registered age of the SIM card holder, without however being certain that the actual user of the SIM card is a minor or an adult.** In the case of fixed network browsing, the Operator would have no way of tracing the age of the user who relies on the IP address of the fixed network (e.g., via Wi-Fi or Ethernet cable). This is because all fixed network contracts are, by definition, registered to adult customers. Another possibility, explains the operator, is verification via Parental Control, which, when active on the device, allows access to sensitive content to be filtered at the network and application level (e.g., via DNS blocks or IP blocks). Verification via Parental Control would be carried out by querying the internal databases of [**OMISSIS – An operator],** i.e., by checking whether Parental Control is active or not on the number requesting access. However, in line with what has already been discussed above, even when Parental Control is used as an *age verification* mechanism, a distinction must be made between mobile and fixed network browsing, as the system is activated directly on the SIM card. In the case of mobile network browsing with a Junior SIM card, Parental Control is pre-activated by default and therefore the minor user is always protected, as this mechanism prevents access to the platforms in question. In the case of a non-Junior SIM card, it is the responsibility of the minor's parent to activate Parental Control on the minor's device. Therefore, age verification via Parental Control would only be effective in the case of underage users who are registered as holders of a Junior SIM card, for whom the use of the Parental Control mechanism is mandatory. On the contrary, [**OMISSIS – An operator]** explains that it would have no way of determining whether the user – a user of a SIM card registered to an adult but without Parental Control active – is actually an adult or a minor. Instead, they point out that in the case of fixed network browsing, since fixed network users are all registered to adults, it will be the responsibility of the minor's parent to activate Parental Control mechanisms on the fixed network and, therefore, minors will automatically be blocked from accessing platforms with pornographic content in all cases where Parental Control is activated on the fixed network by the contract holder. Conversely, minors will be guaranteed access to the site/platform in all cases where the fixed network holder (adult) does not activate Parental Control on the fixed network. Furthermore, it should be noted that the operator will have no way of verifying the age of the user and distinguishing between an adult and a minor using the fixed network (via Wi-Fi or Ethernet cable).

B. Assessments by the Authority

The Authority takes note of the proposal of the GARANTE PER L'INFANZIA (Italian Data Protection Authority for Children) whereby it considers that the adoption of a system based on the use of a SPID-type digital identity would ensure a high degree of certainty in determining the age of the user while respecting the principle of proportionality. This solution could be appropriate where providers make available an additional 'age verification' function with a guarantee of anonymity with respect to the websites and platforms to which the user needs access.

It is also noted that associations and private providers, WEBGROUP, AYLO, and META, believe that ***age verification*** **should be carried out more efficiently at the user's device level, for example in the form of filtering software (APP), rather than at the website level (the Spanish case is cited as an example). In other cases, it is proposed to verify age on users' devices at the operating system level,** although it is recognized that this approach requires the **cooperation of operating system manufacturers. One respondent in particular believes that age verification should be carried out directly at the (virtual) location where teenagers download the application itself (app store or at the operating system level).**

In this regard, from a legal point of view, the Authority notes that the regulatory framework governing age verification systems, and most recently Decree-Law 123/2023 as converted into law, does not impose an obligation on terminal providers, app stores, operating systems, or browsers, but rather on website providers and video-sharing platforms. With regard to the data security risks feared by WEBGROUP, the Authority points out that the approach proposed in the public consultation does not provide for any transfer of personal and sensitive information to the website or platform. Age verification is, in fact, carried out by the certified entity that already possesses the user's data (independent third-party model).

With regard to the observation that it would be sufficient to rely on the parental control systems provided by the operating systems of the terminals, the Authority refers to the provisions of the resolution.
No. 9/23/CONS as well as in Article 13 of Decree-Law 123 of 2023, as converted into law. In general, electronic communications service providers and terminal providers are already required to implement a *parental control* system. However, the legislator has nevertheless decided to provide for an *age verification* system implemented by website and video sharing platform providers, among others, in line with the provisions of the TUSMA and the DSA referred to above.

The Authority nevertheless considers the proposed solutions based on operating systems, browsers (as in Spain), and the labeling of website content to be interesting, and does not rule out that they may contribute to creating a safe *online* environment for minors in the future. In this regard, the Authority considers it appropriate to set up a technical committee to monitor technical solutions, with the collaboration of all institutional and private entities potentially involved. However, this measure must be anchored to current legal provisions that impose protection obligations on website providers and video sharing platforms, with the caution of establishing rules that are proportionate and respectful of users' personal data.

The Authority therefore confirms the provision for an age verification system implemented by the video sharing platform or website operator on the basis of the model proposed in consultation, which excludes the transfer of user data to the platform or website visited.

With regard to the request by some respondents who believe that the Authority **should provide a list of controlled/certified AV service providers, the following is stated.**

The Authority considers it appropriate to point out that any website or platform that falls within the subjective and objective scope of application of this provision, or that voluntarily decides to apply these technical specifications (as clarified in the section on the scope of application), must identify the entity that is able to provide certified proof of age in compliance with legal requirements.

For the purposes of supervision, the Authority considers it appropriate to follow an approach similar to that used in Resolution No. 9/23/CONS, in this case with reference to the companies used by operators to identify the sites and domains to be filtered.

It is therefore established that providers of websites and platforms that disseminate pornographic content, pursuant to Article 13 bis of Decree-Law 123/2023, as amended upon conversion into law, must notify the Authority of the third parties entrusted with age verification, together with a detailed report describing their expertise, the age verification methods used, and the reasons for their selection.

V. ON THE FREEDOM OF CHOICE OF AGE VERIFICATION SYSTEMS BY REGULATED ENTITIES

A. Comments from institutional entities, operators, and associations

The **CNU** welcomes the fact that the entity required by law to choose the age verification tools to be implemented in its service, using a tool that is as non-invasive as possible to achieve the set objective, and to demonstrate the effectiveness of the tool used in accordance with the requirements set by the Authority, also in compliance with the principle of accountability provided for by the GDPR.

ALTROCONSUMO considers it appropriate for the Authority to limit the scope of choice for regulated entities to a **maximum of three** age **verification systems** previously selected by it on the basis of the principles and requirements established, as it argues that leaving the choice between such dissimilar systems and processes to the full discretion of the entities concerned – and which involve a difference in terms of security and guarantees – would lead to unreliable results and unequal treatment of users.

[OMISSIS – An operator] agrees that regulated entities should be able to choose which *age verification* method to implement, provided **that,** following this procedure**, a set of different methods deemed compatible with the**

principles and requirements established by this Authority. It is the operator's opinion that **the Authority should provide regulated entities with a "range" of options for age verification, leaving it up to the individual site/platform to choose which *Age Assurance* service to use on a case-by-case basis, based on specific contractual agreements with the relevant providers.**

B. Authority assessments

The Authority notes that respondents agree with the approach proposed in the consultation, whereby video sharing platform and website providers are responsible for selecting the appropriate age verification system that complies with the provisions of this measure.

However, the Authority does not consider it appropriate to indicate a limited range of systems deemed mandatory, as this could currently represent a disproportionate measure that does not comply with the general principles of technological neutrality and freedom of enterprise.

VI. ON ISSUES RELATING TO THE PROTECTION OF PERSONAL DATA

A. Comments from institutional entities, operators, and associations

AYLO emphasizes that Article 9(1) of the GDPR considers all personal data relating to the sexual orientation of a data subject to be a special category of personal data and that such personal data is particularly sensitive. As such, it enjoys special protection under the GDPR, i.e., the requirement that data must be limited to what is necessary must therefore take on significant value in the case of processing involving sensitive personal data. It considers that, given the absolute lack of proven benefits in relation to the use of strict identity certification/age-gating systems at the website level, **it is neither appropriate nor relevant nor supported by a principle of necessity within the meaning of Article 5 of the GDPR to assume that users' personal data can be collected and stored every time a user visits an adult content website, and this is all the more true in light of the fact that the data processed in this specific case is highly sensitive,** as it relates to an individual's consumption of sexually explicit content. If such data were to become public, this could have significant consequences for their family, social, and professional lives. Identity certification systems can substantially undermine the right of website users to self-determination with regard to their own data. The data collected through such systems significantly increases the risk of *hacking* of such data. Furthermore, the risk of hacking identity certification systems particularly affects vulnerable groups such as the LGBT+ community. In addition, the normalization of the practice of **uploading personal data to access websites carries significant risks, as it can lead to privacy violations, identity theft, and unauthorized use of sensitive data, highlighting the importance of safeguarding personal data in the digital age.**

Assigning this responsibility to the platform or platforms visited by a user means that users repeatedly submit private information to access different adult sites, normalizing the disclosure of personal data on the Internet and creating a risk of potentially irreparable global data identity theft. **With regard to privacy issues, it considers that operating systems now offer users the possibility to limit the collection of browsing history and other data, providing a level of privacy protection that is managed directly by the user.** This autonomy is absent in website-level age verification systems, which often operate with opaque data retention and use policies. In conclusion, it believes that **age verification systems implemented at the device level and** age estimation would offer a more secure and privacy-friendly method, aligning with the principle of data minimization and giving users greater control over their personal information.

WEBGROUP believes that, to date, there is no *age verification* system capable of guaranteeing the protection of users' privacy. Sharing one's identity for the purpose of accessing an adult website inevitably leads to the linking of any user's identity to their presumed sexual orientation or preference, which is the quintessential violation of privacy and exposes them to high risks, including national security. Instead, it argues that **device-level user verification via filtering software avoids these problems because it minimizes the amount of data shared and** does not associate it with the individual's access to pornographic websites, and no data other than that normally collected to configure a device is collected. Furthermore, this data is not stored or shared online, but kept locally on the device, maintaining optimal privacy. Regardless of how it is performed, *age* verification—whether through (i) the direct collection of identity documents by the publisher of the pornographic site; (ii) the estimation of age based on the Internet user's browsing history;
(iii) the processing of biometric data for the purpose of identifying or authenticating a natural person (e.g., by comparing, through facial recognition technology, a photograph shown on an identity document with a self-portrait or selfie); or (iv) **through the use of digital IDs, such as SPID, provided in the public** sector—constitutes **a violation of privacy** where the technology is limited and not advanced enough to protect and preserve fundamental rights. In fact, requiring websites to engage in AV or use third-party AV providers creates repositories of highly sensitive and personally identifiable information, which are lucrative targets for hackers. In **this regard, it notes that dual anonymity AV mechanisms are an interesting but not yet mature option and** that, once properly developed and tested, authorities should create certifications to screen the service providers deemed most secure/efficient, not in a single country or a selection of countries, but in a coordinated manner and at least throughout the European Union.

ALTROCONSUMO believes that certain age verification systems, including those involving the direct collection of documents or the processing of biometric data, should be excluded. **It does not see any particular problems with the use of digital identities such as SPID**, as this is a proven and secure recognition and verification system. As for age estimation based on browsing history, it believes that the person called upon to verify would find themselves using

personal data that is already potentially processed in profiling operations carried out by the person themselves or by third parties, so it does not see any particular critical issues in the use of the tool itself but considers it essential to put in place pseudonymization measures that do not allow the identity of the minor to be traced but only detect statistically recurring elements in the browsing of minors.

B. Assessments by the Authority

The Authority notes that **some respondents, representing video sharing platform and website providers, believe that uploading personal data to access such platforms and websites entails significant risks, as it may lead to privacy violations, identity theft, and unauthorized use of sensitive data.** Therefore, they believe that **age verification systems implemented at the device level** would offer a more secure and privacy-friendly method, aligning with the principle of data minimization and giving users greater control over their personal information.

In this regard, respondents believe that double anonymity AV mechanisms are an interesting option but not yet mature and that, once properly developed and tested, authorities should create certifications to evaluate the most secure/efficient service providers, not in a single country or a selection of countries, but in a coordinated manner and at least throughout the European Union.

A consumer association does not see any particular critical issues in the use of digital identities such as SPID, as it is a proven and secure recognition and verification system.

The Authority shares the opinion of the respondents that it is not **appropriate, pursuant to Article 5 of the GDPR, to assume that users' personal data can be collected and stored every time they visit a platform or website with adult content, and this is all the more true in light of the fact that the data processed in this specific case is highly sensitive**. I n this regard, precisely because of the risks to the protection of personal data highlighted, the Authority considers it appropriate to confirm the adoption of a system based on age verification by a certified independent entity without the transfer of personal data to the content provider.

As mentioned, interest remains in systems based on age verification and filtering at the device level, although such systems fall outside the scope of this provision, which establishes the process and system specifications that remain the responsibility of providers of video sharing platforms and websites that disseminate pornographic content.

It should be noted that, for the purposes of implementing the provisions of Article *13-bis* of Law No. 123 of November 13, 2023, the SPID system does not **fully comply with the technical specifications set out in Annex A (essentially in the part where so-called double anonymity is required)** when the *Service Provider's* authentication request, which contains the domain name of the visited site, is transferred to *the Identity Provider*. Therefore, as illustrated in Annexes A and B, it requires appropriate adjustments.

In this regard, the Authority considers it appropriate to include, among the systems suitable for *age assurance* purposes, solutions based on the Digital Wallet referred to in the preamble to the measure adopting the technical specifications. This is because the technical solutions are being examined by the European Commission task force and, at the same time, meet the requirements of privacy protection, as they do not involve the uploading of user data to the visited site or platform, and of harmonization of solutions at European level. The solution also uses a specific application installed on the user's mobile phone, which allows only the age attribute (i.e., proof of legal age) to be shared with the platform/website as part of the digital identity information. It is believed that this solution addresses the concerns raised by institutional and private respondents.

VII. ON THE INTERVENTION OF INDEPENDENT THIRD PARTIES

A. Observations by institutional entities, operators, and associations

The **GARANTE PER L'INFANZIA (Italian Data Protection Authority for Children)** believes that **the use of third parties, other than those who manage websites and online platforms, to verify the age of users and issue a certified digital identity offers several significant advantages**. It believes that this approach helps to ensure a higher level of impartiality and reliability in the age verification process, as entities that are external and independent from online platforms can operate with a greater degree of transparency and objectivity, minimizing the risk of conflicts of interest or manipulation. Furthermore, as specialized entities, they can be subject to strict data protection rules and regulations and, at the same time, promote greater consistency and uniformity in the age verification process across different online platforms and services. All of this can help ensure that minors are protected in a uniform and consistent manner in all areas of the digital world.

The **CNU** considers **it entirely consistent with the objectives of proportionality, personal data protection, and security to delegate** the issuance of certified "proof of age" **to independent third parties** (whether they are service providers specializing in the provision of digital identity or an organization that has identified the Internet user in another context, such as a bank, public administration, etc.). It therefore agrees that it should not be the websites and platforms subject to the age verification obligation that carry out the verification operations directly. It considers it appropriate that once the certified proof of age has been issued, it should be provided to the user so that they can access or not access the requested content on the website or platform visited. It emphasizes the appropriateness and risk minimization of this method of verifying the age of users, as the entity issuing the proof of age does not know the specific website or platform that the user wishes to visit, and at the same time, the website or platform visited will acquire the proof of age without knowing the user's identity, as no user identification data will be transmitted. The CNU also emphasizes the sensitivity of the additional step through which sites and platforms interact with the independent third party, as it is desirable that providers of

content providers equip themselves with clear and appropriate tools for acquiring and implementing age verification systems, in order to decipher signatures and establish their authenticity.

The **FAF** believes that the most common objection to the adoption of *age verification* systems is the violation of the privacy of those who connect, who would be obliged to disclose their personal data contained in an identity document. To overcome this problem**, a viable solution is to use a third party** to guarantee the security of such data (based on the SPID model). It emphasizes that this is certainly a more challenging option in technological and economic terms, but if it is the only way to get all the parties involved to agree, it should definitely be promoted.

ALTROCONSUMO emphasizes the importance of having authoritative third parties and recommends entrusting the certification function to entities that already deal with identification and certification, such as companies that provide digital identity, digital signatures, and certified email, so that each user can choose which entity to turn to for 'proof of age'. **It therefore suggests adding the 'proof of age' service to those already provided by digital identity, digital signature, and certified email providers**, since users of one or more of these services have already been identified, and 'proof of age' can be issued automatically in the personal area.

[OMISSIS – An operator] agrees that the principle of supplier independence should be used, **as this mechanism** also **meets** the requirements of the GDPR, minimizing the amount of data retained by sites/platforms offering pornographic content and preventing the independent third party from becoming aware of the site/service the user wishes to access. It also considers it essential to define a regulatory framework that allows regulated entities to choose which *Age Assurance* method to use and that does not place the obligation to ensure the protection of underage users on electronic communications operators. **Therefore, it is willing to assume the role of an independent third party, in line with what was proposed in the public consultation.** Nevertheless, for the reasons set out above, it considers that the provision of *age verification* services **by electronic communications operators should be offered on a voluntary basis and only in return for financial remuneration from regulated entities.** Finally, it considers it necessary to impose a technical period of at least 12 months to allow for adaptation to the new provisions and for technical implementation, starting from the date of publication of the final measure following the public consultation. It also believes that where TLC operators are identified as independent third parties who decide at their discretion to offer such *age verification* services, it should be specified immediately in the sector legislation that the necessary *age verification* activities are adequately and systematically remunerated by regulated entities on the basis of commercial agreements. It would be paradoxical if, in view of the obligation imposed on regulated entities, the costs/investments incurred by the providers of the relevant technical solutions to meet these obligations were borne by the latter. In fact, at a technical level, the Operator would have to equip itself with a system that is not currently available – which will require investments as well as recurring costs – in order to process each request from regulated entities. It argues that this service should be considered,

for the independent third party, a commercial service that the Operator is free to choose whether to offer on the market on the basis of commercial agreements with regulated entities in the face of a regulatory requirement to pay a fee.

AYLO declares that it is not in a position to assess the activities of third-party suppliers, but believes that the issues relating to age verification or estimation systems implemented at website level are the same, regardless of whether their operation is the responsibility of the platform or a third-party supplier. Such third parties, in fact, just like the platform, would be obliged to carry out disproportionate data processing activities. It argues that, for the same reasons related to the sensitivity of the information collected, this type of service could not even be reasonably delegated to third parties controlled by public bodies or otherwise subject to public authorization. **Nevertheless, it considers it necessary to involve third parties that develop operating systems ("SSOs").**

B. Assessments by the Authority

The Authority notes the general agreement among institutional respondents and operators on an approach based on a certified or certifiable third party.

It is noted that some suggest adding the 'proof of age' service to those already provided by digital identity, digital signature, and certified email providers, since users of one or more of the above services have already been identified, and 'proof of age' can be issued automatically in the personal area.

We do not agree with the observation made by the representative of platform/website providers that the issues relating to age verification or estimation implemented at platform/website level are the same, regardless of whether their operation is the responsibility of the platform/website or a third-party provider. In fact, these third parties, just like the platform/website, would be obliged to carry out disproportionate data processing activities. In fact, the Authority has clarified in this regard that the third party is normally already in possession of user data for all purposes provided for by law. This would involve adding the age attribute to the digital identity information to be shared when accessing the platform/website.

In light of the favorable positions expressed by the institutional respondents and the issues relating to the protection of personal data raised by other respondents, the Authority confirms the need for a system based on the presence of a certified third party, including digital identity system providers.

The Authority considers, as already mentioned, that the intervention of a private entity, such as an electronic communications operator, as a third party should be based on the provision of services subject to commercial negotiation, as telephone operators are not subject to the legal obligation to verify age.

In the context of an architecture based on a third party, the Authority agrees that one of the possible options is to add the "proof of age" service to those already provided by digital identity, digital signature, and certified email providers, since users of one or more of the aforementioned services have already been identified, and "proof of age" can be issued automatically in the personal area.

With regard to the request to allow a 12-month implementation period, the Authority notes that the timeframe granted for the implementation of the systems referred to in this provision is established by paragraph 4 of Article 13 bis cited above.

VIII. ON THE SUBJECT OF SYSTEM SECURITY

A. Comments from institutional entities, operators, and associations

META believes that collaboration across the entire sector on this issue would ensure safe and age-appropriate experiences, while also preventing young people from migrating to apps that are less secure than those that have invested in security and age-appropriate experiences.

AYLO believes that website-level age verification and age estimation systems would cause significant harm, violate data protection principles, and pose a huge risk to the right to self-determination of website users, creating unnecessary hacking risks due to the large amount of highly sensitive personal data that would need to be collected from users. It highlights that personal data is attractive to malicious actors, so the risks of phishing attacks, identity theft, data breaches, and fraud increase as users share their information with more and more websites and online age verification and estimation service providers. **It emphasizes once again that the best solution to mitigate security risks and circumvention methods in *age assurance* systems is to adopt a device-level method.** This means that users would be verified only once, through their operating system, and not on every age-restricted website. This would drastically reduce privacy risks and create a process that is very simple for regulators to enforce and for users to follow: over 95% of devices worldwide are powered by operating systems owned by three companies. AYLO argues that once age verification and estimation is carried out for the first time on the device by the companies that develop operating systems and device manufacturers, which already hold their users' personal data, users would not be encouraged to share their personally identifiable information multiple times on various sites. **In addition, verification mechanisms implemented at the device level can offer greater security and reduce the risk of unauthorized access or data breaches.** By locating age verification within the device, processing is isolated from the myriad vulnerabilities associated with online platforms, including hacking and phishing attempts. Finally, it believes that with a device-level solution, there would also be no risk of internet traffic diversion, i.e., the risk that users who do not want to reveal their personal information to access a website would move from compliant sites to less secure and non-compliant ones.

WEBGROUP believes that **any device-level *age verification* solution is more secure than third-party systems**. Furthermore, *age verification* implemented directly by platforms risks giving parents a false sense of security, influencing and compromising parental monitoring of minors and their online activities. It is also likely to induce users, including minors, to venture into unregulated parts of the web, including the dark web, risking exposure to more extreme explicit content, including criminal content, and causing problems far more serious than those that *age verification* imposed on platforms was intended to address. Furthermore, it considers that age verification should only be required when a new user logs on to a personal device. Additional verification may also be required when internet browsing data indicates that the device is being used by someone other than the owner, or in cases of suspected identity theft or misuse.

It also argues that one of the negative aspects *of age verification* imposed on platforms is that such verification is not limited to the user's terminal, given the international nature of the internet and data traffic. **Device-level** *age verification* takes place on the user's device, regardless of the geographical origin of the website or its adult content, which also affects the use of VPNs, and **circumvention is much less easy with verification systems limited to the user's terminal.**

ALTROCONSUMO believes that the self-declaration method is insufficient to certify the user's age for obvious reasons, which are also confirmed by the evasive practices recorded in the use of certain social platforms by younger users (e.g., TikTok). Furthermore, it believes that if the *age assurance* system provides for age verification based on estimation, it is necessary to set up a double-check mechanism by the site/platform through a request for documentary evidence. It points out that this type of mechanism must be accompanied by the necessary safeguards and responsibilities regarding the processing of personal data. With regard to the frequency of age verification, it considers that, **if the certification function were entrusted to digital identity, digital signature, and certified email providers, a system of requests could be set up for each access.**

B. Assessments by the Authority

The Authority notes that the platform and website providers who responded on the issue of security believe that the best solution to mitigate security risks and circumvention methods in *age assurance* systems is to adopt a device-level method. **In addition, verification mechanisms implemented at the device level can provide greater security and reduce the risk of unauthorized access or data breaches.**

They note that **device-level** *age verification* takes place on the user's device, regardless of the geographical origin of the website/platform or its adult content, which also affects the use of VPNs, and **circumvention is much less easy with verification systems limited to the user's terminal.**

The consumer association believes that if the certification function were entrusted to digital identity, digital signature, and certified email providers, a system could be set up to request verification at each access.

The Authority shares the concerns of respondents belonging to the category of platform and website providers regarding the data security risks associated with sharing such information over the Internet. As mentioned, terminal-level verification solutions appear interesting but fall outside the scope of this proceeding, which concerns providers of video sharing platform and website services.

With regard to security, the Authority considers that the system adopted in this measure, which is potentially based on a public and private key encryption system or, in any case, on secure connections, provides ample guarantees, although no one can rule out the possibility of circumventing the solutions identified in the IT sector. Similarly, models based on digital identity, such as ID Wallet, are characterized by security requirements as they do not involve the transfer of personal information over the network.

IX. ON THE CRITERIA OF ACCURACY AND EFFECTIVENESS

A. Comments from institutional entities, operators, and associations

META believes that regulations should take into account the efforts and good faith demonstrated in the development and implementation of increasingly effective age verification solutions, and that, ultimately, **this should be done at the operating system level to make the process as simple, consistent, and effective as possible**. Furthermore, it is of the opinion that, despite the efficiency of age verification systems, online users may still misrepresent their age and access services and applications that are not designed for them. For this reason, it advocates a multi-pronged, multi-layered approach that combines different tools to facilitate age-appropriate experiences.

While **AYLO** appreciates the Authority's willingness to collect metrics on the accuracy and effectiveness of age verification mechanisms and to set specific thresholds, it believes that providing definitive recommendations on these issues is beyond its remit and trusts in the Authority's ability to assess and decide on these parameters, emphasizing the need for **measures that balance effectiveness with the principles of privacy and user data protection, while also taking into account the risks we have highlighted regarding any age verification or age estimation solution implemented at the website level.**

ALTROCONSUMO believes that the verification system should focus not so much on the access device as on the content accessed and sent. In fact, it believes that, at present, it is too easy to post a video on social media that could violate privacy, decency, or even security rules. However, it argues that using a universal gatekeeper that only blocks access, according to an "all o r nothing" principle, does not solve the problem, a n d that rather there should be

They would like increasingly sophisticated (and stringent) control systems depending on the activity to be carried out online. He also points out that controlling a cell phone is perhaps easier than controlling a PC (partly because each mobile device corresponds to a registered user), whereas with a PC it is only possible to trace the IP address, which can also be easily masked or falsified. Furthermore, there is a different mode of access: on PCs, the browser is usually the gateway to all internet services, while on mobile devices, apps are often used, and this, in turn, requires two different approaches to the problem of how to control access, each with its own specificities.

WEBGROUP argues that, in general, in the case of platforms offering exclusively adult content, it would be **much more effective to implement AV at the device level using filtering software**. Furthermore, from an effectiveness standpoint, it believes that only platforms established in Italy are subject to the obligations established by the law of the country of origin, leaving the vast majority of the most trafficked pornographic sites not subject to age verification requirements. However, filtering software on devices can prevent minors from viewing all adult content, not just that published in Italy, and therefore educational campaigns on the use of available filtering options could be more effective and much less invasive of freedoms and privacy than the *age verification* requirements imposed on providers.

B. Assessments by the Authority

The Authority notes that no specific quantitative assessments have been provided on the accuracy and effectiveness requirements of the age verification systems described in the public consultation document, and therefore refers to the documentation available in the literature and referred to in the measure.

X. ON THE CRITERIA OF ACCESSIBILITY, EASE OF USE, AND NON-DISCRIMINATION

A. Comments from institutional entities, operators, and associations

[OMISSIS - A video sharing platform provider] believes that it is important to bear in mind that, in the context of age assurance tools, the more specific and granular the information requested by the provider, the greater the impact on the user in terms of personal data collection and *user experience*. The application of data-intensive methods not only increases the risk to data security, but can also discourage users from legitimately accessing services. For example, the use of methods based on age verification through the provision of an identity document can lead to a deterioration in *the user experience*, as well as the sharing of unnecessary personal information, particularly if required in the context of a non-risky service such as, for example, a website for learning a new language online. Furthermore, when balancing the various rights, it is important to consider the diversity of users' needs and characteristics. Since not everyone has a credit card or identity document, verifying age using only rigid identifiers would risk excluding certain categories of people.

marginalized or from socio-cultural contexts disadvantaged in terms of access to services and information, thus contributing to widening the cultural and economic divide. Furthermore, **[OMISSIS**

- A video sharing platform provider] believes that *age assurance* mechanisms should require maximum commitment from the industry to ensure that the solutions provided are simple and effective, including in the context of supervision by parents and guardians. Only in this way will it be possible to promote user confidence in the process, while ensuring the effective protection of minors from adult content.

The **CNU** highlights the importance of the criterion relating to the ease of use and accessibility of the *age assurance* system, which must be respected by regulated entities in order to ensure that the age verification system is easy to use for all users, regardless of their characteristics, and above all that it is accessible to users with disabilities, ensuring, , for example, that screen readers can be used to successfully complete the verification process.

ALTROCONSUMO points out that, as with digital identity, which is mandatory for citizens, a similar tool should not raise any particular issues in terms of accessibility and that minors in particular have a medium/high level of computer literacy. Conversely, for those who are less computer literate, as with digital identity, there are more analog channels such as activations at physical counters/stores that can also be used to certify age. With regard to the criterion of inclusiveness and non-discrimination, it considers that if the verification system leads to inaccurate or erroneous results, a review procedure could be envisaged at the request of the person concerned or the website/platform for a more accurate verification based on reliable data. For example, if the estimation system were to classify an adult as a minor, the adult could resort to the review procedure by presenting an identity document. Conversely, if the website/platform were to consider the *age assurance* on a minor to be false, it could request documentary proof of age from the user.

B. Assessments by the Authority

The Authority agrees with the observation that the more specific and granular the information requested by the provider, the greater the impact on the user in terms of personal data collection and *user experience*. The application of data-intensive methods not only increases the risk to data security, but may also discourage users from legitimately accessing services.

The Authority therefore favors the adoption of systems that are secure but, at the same time, easy for citizens to use.

XI. ON THE CRITERION OF TRANSPARENCY

A. Comments from institutional entities, operators, and associations

AYLO fully supports fully the spirit of the Authority aimed at a greater transparency, regardless of the age verification or estimation system used, and believes in the need for

provide users, both adults and minors, with clear and comprehensive explanations of any type of processing carried out on our platforms.

WEBGROUP reiterates that **age verification should be limited and performed on the personal device** and, subsidiarily, the user should be informed to the extent required by data protection laws (GDPR), which would probably involve requesting the user's consent for the third party to become aware of their personal identity and age, exclusively for the purposes of age verification and excluding any other personal data, including knowledge of any of the user's Internet activity. To the extent required by law, the user should also be informed that the independent third party is certified by a certification authority, whose role would be to organize the operation of age verification by the third party by providing cryptographic specifications for the service and to certify third parties (with the possibility of revoking third parties if necessary).

ALTROCONSUMO believes that infographics and tutorials used by regulated entities, the Authority, and certification bodies are a means of promoting transparency.

B. Authority assessments

The Authority agrees with the observations regarding the need for maximum transparency towards users.

XII. ON THE SUBJECT OF TRAINING AND INFORMATION

A. Comments from institutional entities, operators, and associations

AYLO maintains that the press, blogs, and websites are useful tools for promoting the importance of age verification and estimation and for raising awareness of the dangers and risks associated with the Internet. AYLO states that it has been dealing with *age assurance* mechanisms for many years and has conducted awareness-raising activities with the press and also through our websites regarding the dangers associated with age verification and estimation tools implemented at the website level. Furthermore, it states that the login page to its websites also includes a disclaimer and a request for self-declaration of age aimed at discouraging underage users from visiting the sites. In addition, it believes that technical measures alone are almost never sufficient to solve social problems on their own and that adequate and effective protection of minors can never work meaningfully without the participation of parents. For this to happen, it is of the opinion that parents must first be able to participate in a meaningful way and that they should be trained as comprehensively as possible on the typical behavior of children and adolescents on the Internet. In particular, they should be informed about how their children use the Internet and what the associated dangers and opportunities are. Finally, it welcomes any efforts by the Authority to improve the training of parents in this regard.

The **CNU** believes that only through a series of measures, not only legislative and regulatory, but also in the areas of communication and digital education, will it be possible to make a concrete contribution

to ensure effective age verification and, therefore, increasingly effective protection of minors from the risks of the web.

The **GARANTE PER L'INFANZIA (Italian Data Protection Authority for Children)** believes that, beyond technical solutions, extensive education and awareness-raising on digital issues remains essential with regard to the protection of the physical and mental health of minors online. This initiative should be carried out in advance and in parallel with the introduction of new technical tools, using all available channels of information and training, activating all appropriate institutional synergies and, above all, actively involving minors themselves in the decision-making process regarding online protection policies, listening to their experiences, opinions, and concerns in order to help develop *age assurance* measures that are more effective and respectful of their rights and desires.

ALTROCONSUMO believes that consumer representative associations are a valid channel for dissemination.

B. Assessments by the Authority

The Authority certainly agrees with the respondents' comments on the need for adequate training and information for minors and their parents.