

**RESOLUTION NO. /24/CONS**

**ADOPTION OF TECHNICAL AND PROCEDURAL ARRANGEMENTS FOR  
ASCERTAINING THE AGE OF MAJORITY OF USERS PURSUANT TO  
LAW NO 159 OF 13 NOVEMBER 2023**

**THE AUTHORITY**

AT THE Council meeting of 2024;

HAVING REGARD TO Law No 481 of 14 November 1995 on *‘Rules relating to competition and the regulation of public utility services. Establishment of regulatory authorities for public utility services’*;

HAVING REGARD TO Law No 249 of 31 July 1997 on *‘Establishing the Communications Regulatory Authority and laying down rules relating to the telecommunications and radio-television systems’*, hereinafter the *Authority*;

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

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

HAVING REGARD TO Legislative Decree No 259 of 1 August 2003, laying down the *‘Electronic Communications Code’* (hereinafter also referred to as the *‘Code’*), as last amended by Legislative Decree No 48 of 24 March 2024, laying down *‘Corrective provisions for Legislative Decree No 207 of 8 November 2021, for the implementation of Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018, amending Legislative Decree No 259 of 1 August 2003, laying down the Electronic Communications Code’*;

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

HAVING REGARD TO Legislative Decree No 208 of 8 November 2021, on the *‘Implementation of Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 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 changing market realities*’, as amended by Legislative Decree No 50 of 25 March 2024, containing ‘*Supplementary and corrective provisions for Legislative Decree No 208 of 8 November 2021 on the consolidated text of audiovisual media services in view of changing market realities, implementing Directive (EU) 2018/1808 amending Directive 2010/13/EU*’.

HAVING REGARD TO Decree-Law No 123 of 15 September 2023 on ‘*Urgent measures to tackle youth hardship, educational poverty and child crime, as well as child safety in the digital environment*’ as converted, with amendments, by Law No 159 of 13 November 2023 and, in particular, Articles 13a 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 19 October 2022 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Regulation, hereinafter also DSA);

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

HAVING REGARD TO Resolution No 298/23/CONS of 22 November 2023 on the ‘*Regulation implementing Article 41(9) of Legislative Decree No 208 of 8 November 2021 on programs, user-generated videos or audiovisual commercial communications addressed to the Italian public and conveyed by a video-sharing platform whose supplier is established in another Member State*’ and the related notification as a technical regulation to the European Commission;

HAVING REGARD TO Resolution No 9/23/CONS of 25 January 2023 on the ‘*Adoption of guidelines for the implementation of Article 7a of Decree-Law No 28 of 30 April 2020 on “systems for the protection of minors from cyberspace risks”*’;

HAVING REGARD TO Resolution No 223/12/CONS of 27 April 2012, on ‘*Adopting the new Regulation on the organisation and operation of the Communications Regulatory Authority*’, as last amended by Resolution No 434/22/CONS;

HAVING REGARD TO Resolution No 401/10/CONS of 22 July 2010, on *Regulating the time limits for proceedings*, as amended and supplemented;

HAVING REGARD TO Decision No 107/19/CONS of 5 April 2019, on ‘*Adoption of the Regulation on the consultation procedures in proceedings falling under the Authority’s competence*’;

HAVING REGARD TO the Memorandum of Understanding signed on 12 April 2023 between the Authority and the Data Protection Commissioner, in which 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 to political advertising;

HAVING REGARD in particular to the Joint Table set up by the two Authorities, intended to promote a code of conduct that leads digital platforms to adopt systems for verifying the age of young users accessing services *online*;

HAVING REGARD TO Resolution No 9/24/CONS of 10 January 2024, which provided for the *‘Initiation of the investigative procedure aimed at implementing Article 13a of Decree-Law No 123 of 15 September 2023 on urgent measures to combat youth hardship, educational poverty and child crime, as well as child safety in the digital environment, converted, with amendments, into Law No 159 of 13 November 2023’*;

HAVING REGARD TO Article 1 of that resolution and, in particular, paragraph 1 thereof, which initiated the preliminary investigative procedure aimed at implementing Article 13a(3) of Decree-Law No 123/2023, converted, with amendments, into Law No 159/2023, by approving a measure governing the technical and procedural methods that the persons identified by the provision are required to adopt to ascertain the age of majority of users;

WHEREAS paragraph 4 of the same article provides for a 30-day public consultation on the Authority’s decision, after obtaining the opinion of the Data Protection Commissioner;

HAVING REGARD TO Resolution No 61/24/CONS of 6 March 2024, on the *‘Launch of the public consultation referred to in Article 1(4) of Decision 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 13 November 2023’*;

WHEREAS the legislation in force — also specifically referring to the role of the Authority — repeatedly refers to the need to implement age verification mechanisms, establishing that minors have the right to a higher level of protection from content that may impair their physical, mental, or moral development, including by introducing stricter measures against any information society service;

WHEREAS the European Commission supports and promotes the implementation of rules aimed at the protection of minors online and Article 28 of the DSA requires that all online platform providers accessible to minors 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;

WHEREAS, in accordance with Article 35(1)(j) of the DSA, providers of very large online platforms and very large online search engines shall adopt systemic risk mitigation measures, including *‘targeted measures to protect the rights of the child, including age verification and parental control tools, tools aimed at helping minors signal 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 conferred on the Authority by the TUSMA and, in particular:

- Article 41(7), insofar as it provides that: *Without prejudice to Articles 14 to 17 of Legislative Decree No 70 of 9 April 2003, and without prejudice to the provisions of the preceding paragraphs, **the free circulation of programmes, user-generated videos and audiovisual commercial communications conveyed by a video-sharing platform whose supplier is established in another Member State and directed to the Italian public may be restricted, by decision of the Authority**, in accordance with the procedure laid down in Article 5(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(1);*

- Article 42(1) and (6), insofar as they provide that: 1. *Without prejudice to Articles 14 to 17 of Legislative Decree No 70 of 9 April 2003, providers of video-sharing platforms under Italian jurisdiction **must take appropriate measures to protect:***

*a) **minors from programmes, user-generated videos, and audiovisual commercial communications that may harm their physical, mental, or moral development in accordance with Article 38(3);***

*[omitted]*

6. *For the purposes of protecting minors referred to in paragraph 1(a), the most harmful content shall be subject to the strictest access control measures.*

WHEREAS, in particular, pursuant to Article 42(7) of the TUSMA:

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

*[omitted]*

*f) **establish 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 harm the physical, mental or moral development of minors;*

*[omitted]*

*h) **establish parental control systems under the supervision of the end-user as regards content that may impair the physical, mental, or moral development of minors;***

CONSIDERING, therefore, that it is appropriate to assess, in the context of the public consultation launched by Resolution No 61/24/CONS, whether the age verification system outlined in the document put forward for consultation by indicating general requirements and performance indicators is effective, suitable and functional to be applied, in accordance with the regulatory context referred to above, also with reference to other types of content that could harm the physical, mental or moral development of minors;

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

WHEREAS it is appropriate to clarify, in light of the comments made by some of the participants in the public consultation, that the rules governing the technical and procedural arrangements for ascertaining the age of majority of users, which this resolution approves in implementation of Article 13a of Decree-Law No 123/2023 converted, with amendments, into Law No 159/2023, **must be adopted by website operators and providers of video-sharing platforms, which disseminate pornographic images and videos in Italy, wherever they are established;**

WHEREAS, for all intents and purposes, in light of the regulatory framework referred to above and the results of the consultation itself, the technical and procedural arrangements for verifying the age of majority of users, which are approved by this resolution in implementation of the aforementioned decree-law (as converted into law) **are highly recommended, as they are effective, suitable, proportional, and functional, for their own use as well as by entities other than those directly regulated herein and with reference to other types of content, in addition to those of a pornographic nature, which could in any case harm the physical, mental, or moral development of minors, such as the categories provided for by Resolution 9/03/CONS;**

HAVING REGARD TO Decision No 88 of 8 February 2024 by which, pursuant to Article 58(3)(b) of Regulation (EU) 2016/679, the Data Protection Commissioner (Commissioner), having examined the draft measure sent by the Authority, gave a favourable opinion on the launch of the public consultation provided for by the Authority with its Resolution No 9/24/CONS of 10 January 2024;

HAVING REGARD TO Decision No 470 of 17 July 2024 by which, pursuant to Article 58(3)(b) of Regulation (EU) 2016/679, the Commissioner expresses a favourable opinion on the text of the draft measure, transmitted by AGCOM by letter of 12 June 2024 following the conclusion of the aforementioned public consultation, provided that the additions indicated in the separate letter sent with the aforementioned measure are incorporated;

HAVING REGARD TO the fact that, as a technical regulation, the draft measure approved by the Council at its meeting in 2024, on the ‘Adoption of the technical and procedural arrangements for ascertaining the age of majority of users pursuant to Law No 159 of 13 November 2023’, has been notified to the European Commission pursuant to Directive (EU) 2015/1535;

HAVING REGARD TO the outcome of the notification procedure to the European Commission;

HAVING CONSULTED the report by Commissioner Laura Aria, rapporteur pursuant to Article 31 of the Regulation on the organisation and functioning of the Authority;

## HEREBY DECREES

### Single article

1. In the context of the investigative procedure aimed at implementing the provisions of Article 13a(3) of Decree-Law No 123/2023, converted, with amendments, into Law No 159/2023, referred to in Article 1 of Resolution No 9/24/CONS, the rules and technical and procedural arrangements to be adopted by the persons identified by the legislation for ascertaining the age of majority of the users referred to in **Annex A**, which forms an integral and substantial part of this resolution, shall be adopted.
2. The Authority launches a Technical Round Table to monitor and analyse technical, legislative, and regulatory developments in the field of age assurance systems.
3. The Authority shall ensure the correct application of the provisions of this order and its annexes pursuant to Article 13a of Decree-Law No 123/2023 converted, with amendments, into Law No 159/2023, as amended.

This measure shall be published on the Authority's website.

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

Rome, 2024

THE PRESIDENT  
Giacomo Lasorella

COMMISSION SPOKESPERSON  
Laura Aria

Attesting the conformity of the decision  
THE SECRETARY-GENERAL



Giulietta Gamba

## Annex A to Resolution No /24/CONS

### TECHNICAL AND PROCEDURAL ARRANGEMENTS FOR ASCERTAINING THE AGE OF MAJORITY OF USERS PURSUANT TO ARTICLE 13A OF DECREE-LAW NO 123 OF 5 SEPTEMBER 2023, CONVERTED WITH AMENDMENTS INTO LAW NO 159 OF 13 NOVEMBER 2023

This regulation governs the technical and procedural arrangements that the entities specified by the Decree are required to adopt to ascertain the age of majority of users.

## Article 1

### DEFINITIONS

**Age assurance** is the set of methods, systems and processes used to determine an individual's age or age group at varying 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 in 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 a user is likely to be of a certain age, of a certain age group, or above or below a certain age. Age estimation methods include automated analysis of behavioural and environmental data, comparing how a user interacts with a device or other users of the same age, metrics derived from analysis of body movements, facial recognition, or analysis of skills or knowledge. Methods used for estimating age also include those carried out using algorithms and the use of technologies based on artificial intelligence.

**Age verification** refers to those systems that rely 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 (e.g. scratch card) or digital (e.g. electronic document, file, alphanumeric string, electronic transaction, etc.) object that allows the establishment, on the basis of processes and protocols encoded and recognised between the parties, of the age of majority of the user who uses it.

**Regulated service:** the dissemination and/or publication, in Italy, of images and videos of a pornographic nature through websites and providers of video-sharing platforms subject to the obligation to verify the age of the user wherever established in accordance with the provisions of the aforementioned Article 13a. Such content includes advertising content (e.g. banners, pop-ups, *interstitials* etc.).

**Video-sharing platform provider:** the natural or legal person providing a pornographic video-sharing platform service;

**Video-sharing platform service:** a service, as defined in Articles 56 and [57 of the Treaty on the Functioning of the European Union](#), where the principal purpose of the service or a dissociable section thereof is devoted to providing programmes, under the editorial responsibility of a media service provider, to the general public, in order to inform, entertain or educate, by means of electronic communications networks within the meaning of [Article 2\(a\) of Directive 2002/21/EC of the European Parliament and of the Council of 12 July 2002](#) and whose organisation is determined by the provider of the video-sharing platform, including by automated means or algorithms, in particular by displaying, tagging and sequencing;

**Regulated entity:** Website operators and providers of video-sharing platforms, wherever established, who disseminate pornographic images, programmes and videos in Italy, are to be considered subject to the age verification requirement.

**Performance indicators:** qualitative and quantitative parameters that allow for the measurement of the effectiveness of an age assurance system in terms of limiting errors in age determination both in test environments and under 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 rate of *Wrong OKs*, i.e. the rate of *false positives*, in allowing access (i.e. the likelihood that the system will allow access to prohibited content to a minor). Another performance indicator used in some studies is the *mean absolute error* (a measure of the average difference between the actual and the predicted age) which must be within acceptable tolerances.



## Article 2

### **REQUIREMENTS, TECHNICAL SPECIFICATIONS AND PERFORMANCE INDICATORS FOR AGE ASSURANCE SYSTEMS THAT REGULATED ENTITIES ARE REQUIRED TO COMPLY WITH AND ADOPT**

1. The Authority shall adopt an approach that is technologically neutral, leaving the parties responsible for carrying out the age assurance processes, i.e. regulated entities, a reasonable level of freedom of assessment and choice, while establishing the principles and requirements that must be met by the systems introduced.
2. In view of the results of the public consultation and the opinion of the Data Protection Commissioner, in light of the analyses carried out, including at Community level, the Authority establishes that a functional system for providing the ‘Age assurance’ must comply with the **process and system requirements and specifications** described below.

#### **i. Proportionality:**

- This is a general requirement, of a primary nature, which refers to finding the right balance between the means used to achieve the intended objective, in this case age verification, and its impact on the limitation of the rights of individuals. The person required, by law, to implement the age control system for access to content, by means of age assurance, must use as non-invasive a tool as possible to achieve the intended objective.
- In accordance with the principle of accountability pursuant to Articles 5(2) and 24 of Regulation (EU) 2016/679 (‘GDPR’), it is appropriate that the ‘regulated entities’ choose the age assurance tools to be implemented in their service and demonstrate the effectiveness of the tool used according to the principles and requirements set by the Authority, as well as the compliance of the same tool with the principles and rules on data protection, in particular, that of proportionality. In this context, the document also considers the impact of the tool used on the ‘rights of individuals’ 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 27 April 2016 - GDPR (data minimisation, accuracy, storage limitation, etc.). The methods chosen for age verification by

regulated entities must, in particular, comply with the principle of data minimisation (Article 5 of the GDPR) and the principles of *data protection by design* and *by default* (Article 25 of the GDPR).

- Age assurance processes involve the processing and management of personal data such as, for example, data on identity documents, the photographic image of the user, the information of the credit card holder, etc. Therefore, in order to ensure the protection of users' privacy, regulated entities implementing age assurance processes must ensure that the processing of personal data takes place in compliance with the obligations under the GDPR, providing appropriate information to users and ensuring that only the personal data necessary for the purpose is collected.
- The Authority notes that the *parental control* means, referred to in Resolution No 9/23/CONS, which restrict access to content by means of network-wide and application-wide filtering tools, restrict access to sensitive content without requiring the provision of sensitive data.
- The Authority considers that regulated entities and third parties involved in the age assurance process and related processes (e.g. system maintenance, service management or billing, etc.) should not carry out any user profiling and, in particular, the age assurance mechanisms implemented should not allow regulated entities to collect users' identity, age, date of birth or other personal information.
- The Authority does not consider compliant, with respect to the issue of privacy, those systems that are based on:
  - the direct collection of identity documents by the publisher of the pornographic site;
  - age estimation based on the internet user's browsing history on the web;
  - the processing of biometric data for the purpose of identifying or authenticating a natural person (for example, by comparing, using facial recognition technology, a photograph on an identity document with a self-portrait or a selfie).

**In view of the opinion of the Data Protection Commissioner and the related considerations in relation to the possible use of digital IDs provided in the public sphere**, in the context of the possible solutions to be implemented and without prejudice to the need to preserve the freedom of assessment and choice of technology on the part of regulated entities, the following is to be noted.

The use of public databases or an authentication system could theoretically be compliant with these Guidelines only on the condition that its operation does not involve the registration of uses on the servers of State bodies and private companies, as it is not permitted **to make available to those entities a list of connections of a purely private nature and of presumed sexual orientations.**

As explained in section I.8 of Annex B to this decision, the SPID system, for example, does not appear, for the purposes of implementing the provisions of Article 13a of Law No 123 of 13 November 2023, to fully comply with the AGCOM's technical specifications indicated below (essentially in the part where so-called double anonymity is required), at the time of transferring to the Identity Provider the request for authentication from the Service Provider, which contains the domain name of the site visited. That SPID authentication system allows the Identity Provider to know the particular site/platform visited by the user and it is not excluded that this information is stored within the systems of the Identity Provider<sup>1</sup>.

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 the legislation on the protection of personal data, it is nevertheless useful to highlight the usefulness of the security levels offered by the Digital Identity Managers, which, it should be recalled, are third parties themselves (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-specific legislation, selected on the basis of specific qualification procedures and supervised by the Agency for a Digital Italy (AGID)<sup>2</sup>.

It is therefore possible, with a public system, to have a set of certified Identity Providers and a network of connections and agreements (based on existing regulatory obligations) in a short time, able to provide the user, and through this the platform, the so-called proof of age.

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

The Authority, therefore, only if the requirements of the following section on double anonymity are met (protection of personal data against the site/platform and lack of

---

<sup>1</sup> By way of example, the method of authentication *SPID Single Sign On - SP initiated redirect* 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 the purposes of authentication, but through the *User\_agent*.

In the technical documentation of the *SPID Single Sign On* (available at <https://docs.italia.it/italia/spid/spid-regole-tecniche/it/stabile/single-sign-on.html#esempio-di-authnrequest>), however, the exchange of messages containing **metadata** from the *Service\_provider* to the *User\_agent* and from the *Identity\_provider* to the *User\_agent* is provided for, 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.

<sup>2</sup> For example, solely for the 'certification' component, the SPID system has been based, from the outset, on a process of accreditation and supervision of the entities carrying it out.

knowledge of the site/platform visited by the Identity Provider), considers that public systems are usable.

### ***Minimum requirements applicable to all age verification systems***

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

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

A provider of age verification systems must be legally and technically independent from any online service provider covered by this Regulation and must ensure that the services concerned, which disseminate pornographic content, do not under any circumstances have access to the data used to verify the age of the user.

#### **Confidentiality with respect to services disseminating pornographic content**

Personal data, which allow 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 services covered by the regulation to collect the identity, age, date of birth or other personal information of such users.

#### **Confidentiality regarding providers generating proof of age**

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

#### **Confidentiality with regard to any other third parties involved in the age verification process**

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

#### **Enhanced confidentiality regarding services disseminating pornographic content**

An age verification system using ‘double anonymity’, i.e. based on the intervention of an independent third party (section iii below), should not allow the services covered by the Regulation to recognise 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 using ‘double anonymity’ should not allow these services to know or infer the source or method for obtaining the proof of age involved in the process of verifying a user’s age.

An age verification system that respects ‘double anonymity’ should not allow these services to recognize that two proofs of age come from the same source of proof of age.

### **Enhanced confidentiality with regard to entities providing proof of age**

The requirement of *Enhanced confidentiality*, which is in addition to that of the *Confidentiality*<sup>3</sup> above, provides for an age verification system using the ‘double anonymity’ model, where proof of age providers should not be allowed to know for which service the age verification is performed. In particular, in the age verification process using ‘double anonymity’, persons providing proof of age must not be provided with information about the website/platform the user wishes to access.

### **Greater confidentiality with regard to any other third parties involved in the age verification process**

An age verification system using ‘double anonymity’ should not allow any other third party involved in the process to recognise a user who has already used the system. For example, a third party that ensures the transmission of proof of age or certifies its validity should not be able to know if it has already processed the proof for the same user.

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

In general, the Authority considers that an age verification system with two logically separate steps complies with these 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 IN THE USER TERMINAL**

- In this case, an age verification process, capable of providing the necessary degree of protection of personal data, must be divided into three distinct phases:
  - First, the issuance of a ‘proof of age’, with a certain level of confidence, **following the identification**. This proof can be issued by different entities who know the Internet user, whether they are service providers specialized in the provision of **digital identity**, or an organization or entity that has identified the Internet user in another context. **The entity**

---

<sup>3</sup> It is to be noted that the *Confidentiality* requirement, as regards services disseminating pornographic content, provides that personal data, which allow 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 services covered by the regulation to collect the identity, age, date of birth or other personal information of such users.

**providing the ‘proof of age’ shall not be aware of the use the user will make of it.**

The Authority considers it appropriate that sites and platforms subject to the age verification requirement 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 site or platform offering pornographic content. Entrusting these functions to different entities enables maximum protection of the personal data through a process that ensures the compartmentalisation of entities involved, namely between the user, the content provider, and the entity that certifies the age of majority. The Authority considers it necessary that proof of age providers, unless already subject to regulatory user identification obligations, be subject to third-party assessment (i.e. that they are therefore certified to some extent). As mentioned above, in the case of public systems, Digital Identity Managers are themselves ‘third parties’ (both in relation to the regulated entity and in relation to ‘State bodies’ and managers of ‘public databases’) and have certain subjective and objective requirements established by sector-specific legislation, as well as being selected on the basis of specific qualification procedures and supervised by the Agency for a Digital Italy (AGID).

- Second, the provision of that certified proof of age to the user or directly to the site or platform visited in order to grant or deny access to the requested content. The provider of the website or platform does not possess any data on the identity of the user. In case the entity providing the ‘proof of age’ transmits it directly to the site or platform, this is not considered compliant as it implies that the same entity issuing the proof of age will be aware of the particular site 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 this case, the entity 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 identity of the user. Furthermore, in the event that the person responsible for providing 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 appropriate that this be certified by a



designated authority in order to ensure guarantees on the identification system used.

- A third step, implemented by the site or platform visited by the user, consists of analysing the proof of age submitted and providing, or not, access to the requested content (**authentication**).

- Below is an example of the above process:

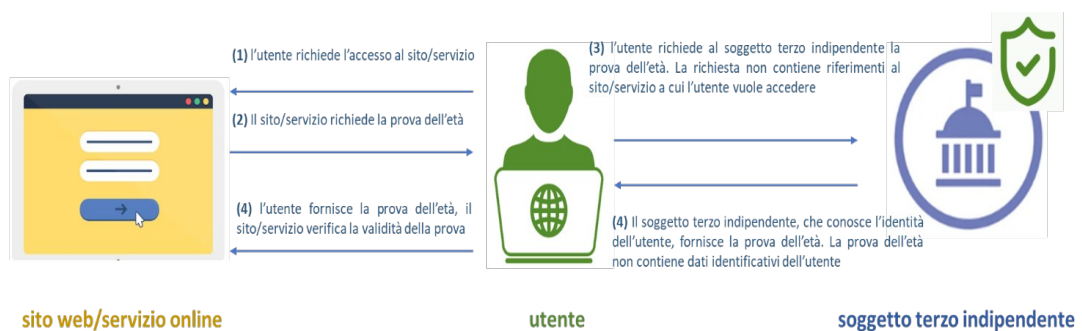
- 1) The entity providing the ‘proof of age’, such as a bank, telephone operator, public body, or private entity (including a merchant) where the user has been definitively identified for other services or for accessing adult content and services, knows the identity of the internet user but does not know which online site/service they are consulting;
- 2) At the request of the user, the third party provides ‘proof of age’ (a type of certification) which is delivered to the user (in the case, for example, of scratch cards), or sent to the user (in the case of an electronic process). This ‘proof of age’ does not contain any data identifying the user or tracing back to the user. For example, in the case of the electronic provision of ‘proof of age’, it is possible to envisage systems that use public and private key encryption to manage the certification and verification as described below<sup>4</sup>:
  - a) — To access the content, the site or video platform requires the user to verify their age and sends an object (e.g. a file or an alphanumeric string) called ‘age to be proven’. **That object does not contain any reference to the website, video-sharing platform or content to which the user wishes to gain access.**
  - b) The user requires the third party to provide proof of age, certifying the item called ‘age to be proven’. The third party certifies the ‘age to be proven’ object by encrypting it with a private key and 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 website or platform they want to access. The site or platform applies decryption using the public key to the ‘proof of age’ to trace the content of the object, after which it 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 re-use or fraudulent creation of certifications.

---

<sup>4</sup> Asymmetric encryption is a form of encryption 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 by 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.

That application presupposes the existence of a Certification Authority responsible for generating, sharing, revoking and managing certificates and encryption keys.

- 3) the website/platform or online service obtains proof of the user's age of majority and, while necessarily knowing the particular online content consulted by the user, has no information about their identity.



sito web/servizio online	website/online service
(1) l'utente richiede l'accesso al sito/servizio	(1) The user requests access to the site/service
(2) Il sito/servizio richiede la prova dell'età	(2) The site/service requires proof of age
(4) l'utente fornisce la prova dell'età, il sito/servizio verifica la validità della prova	(4) The user provides proof of age, the site/service verifies the validity of the proof
(3) l'utente richiede al soggetto terzo indipendente la prova dell'età. La richiesta non contiene riferimenti al sito/servizio a cui l'utente vuole accedere	(3) The user requests proof of age from the independent third party. The request does not contain references to the site/service which the user wants to access
(4) Il soggetto terzo indipendente, che conosce l'identità dell'utente, fornisce la prova dell'età. La prova dell'età non contiene dati identificativi dell'utente	(4) The independent third party, who knows the identity of the user, provides proof of age. The proof of age does not contain user identification data
Utente	User
soggetto terzo indipendente	independent third party

- The Authority stresses the importance of the 'proof of age' containing only information on the user's age of majority and, therefore, not including references to their identity or actual age.

#### AGE ASSURANCE SYSTEMS BASED ON THE USE OF APPLICATIONS

- The third party providing the proof of age shall make available to the user an APP for the certification and generation of the 'proof of age' (e.g. **a Digital Identity Wallet APP, or a 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 through a QR Code<sup>5</sup>. The user, by scanning the QR Code with the camera of their smartphone, accesses, via a link, a service (on the platform/website) dedicated to authentication and will use the APP to send the ‘proof of age’ directly from their device without the intervention of any external web service, ensuring that the confidentiality of the information related to the site/platform/content visited is maintained and that this information is not disclosed to external parties, but is managed exclusively within the user’s device.

- Pursuant to Article 12b(3) of the ‘Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework’, very large online platforms, as defined by the DSA, which require user authentication for access to online services, will also **have to accept the use of European Digital Identity Wallets (EU digital wallets)**, strictly at the voluntary request of the user, including with regard to the minimum attributes necessary for the specific online service for which authentication is required, such as proof of age.

### Obligations to notify the Authority

Website operators and providers of video-sharing platforms, which disseminate pornographic images and videos in Italy, must communicate to the Authority the third parties entrusted with the age verification operation (the independent third party), together with a report containing any useful information on the entity, on the method of age verification and on the reasons for the choice, for the purposes of the supervisory activity under their responsibility.

#### iv. Security:

- The age assurance system must take into account possible cyber attacks, against which it must provide sufficient cybersecurity measures to mitigate risks (the GDPR, the proposed Cyber Resilience Act - CRA) and to avoid circumvention attempts.

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

---

<sup>5</sup> QR Code is the contraction of ‘Quick Response Code’, which is a quick response matrix barcode. It is a symbol that provides data and information to the user whenever it is captured by the camera of a smartphone.

(a) The accuracy, reliability, and risk of fraud of the data source, including consideration of risks associated with the deduction or derivation of 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 circumvention attempts 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-wide 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 (for example, a false driving licence, a forged passport, or a forged registration in a database) or use, in cases of facial recognition, still or video images; It is therefore necessary to provide for techniques to establish the liveness of an individual. Therefore, a so-called liveness detection system, e.g. as defined by ISO/IEC 30107, becomes important;

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

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

As for the means currently offered on the market, several regulators point out that currently all the proposed solutions can be somehow circumvented. For example, the use of a VPN, which was created to ensure security when using the Internet for users, can at the same time allow a minor to circumvent an age verification system. The person required, by law, to implement the age control system for access to content must not promote or refer to any circumvention mechanism of age assurance systems.

v. **Accuracy and effectiveness:**

- The age assurance system must be effective in terms of containing the error in age determination both in the test environment and in real operating conditions. The degree of effectiveness can be determined on the basis of established performance indicators such as, for example, in the case of estimation-based systems, the *average error*, the *standard deviation*, the rate of *Wrong OKs*, i.e. the rate of *false positives*, in allowing access (i.e. the likelihood that the system will allow access to prohibited content to a minor).

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

The age verification mechanism must correctly determine the age of a user under real operating conditions, whether unforeseen or actual, 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 positioning of the user in the image (for methods based on a photographic facial image, or a photo of the identity document, etc.) or even the resolution of the camera.

The age verification mechanism must provide a performance that does not change over time. This could happen with AI-based systems, where population data and demographic characteristics may change over time, leading to a higher degree of variance in the age verification mechanism. This is due to the fact that the data on which the mechanism has been trained become less representative of the population that actually uses it. This element requires continuous monitoring of the degree of accuracy of the mechanism used, making the necessary corrections.

The Authority considers that, similarly to what happens in the electronic communications sector, at the first application stage it is appropriate that each regulated entity, with the support of the service provider, publishes on its website the appropriate performance indicators and the related values that characterise it.

- Self-declaration age assurance is not considered an effective method for correctly determining a user's age.
- The age assurance system shall be neutral or independent of the access device or operating system used by the user.
- Regulated entities must ensure that no user accesses pornographic content until they have demonstrated that they have reached the age of majority, i.e. until the age assurance process is completed.
- The age assurance process must be done each time the website/video sharing platform that disseminates pornographic content is consulted. After the consultation of the service is interrupted, a new age verification must be triggered in the event that the pornographic content is accessed again.
- The validity of an age verification must therefore cease when the user leaves the service, when the session ends, when the user exits the browser, or when the operating system enters 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, user-friendliness and non-obstructive access to content on the Internet:**

- Age guarantee systems must be user-friendly and based on the abilities and characteristics of minors. Age verification should not restrict access to the internet but rather facilitate it by not creating unnecessary obstacles to the use of services and content.
- Age guarantee systems must be accessible. Accessibility means the criterion according to which the age verification system is easy to use for all users, regardless of their characteristics (age, gender, ethnicity, language, etc.), their level of computerisation or the fact that they belong to a certain group (e.g. users with disabilities). Therefore, regulated entities must ensure that the system implemented is user-friendly and does not unduly prevent adults from accessing legal content. This could happen, for example, if the mechanism is too difficult to use, thus causing users to abandon the verification process and therefore the website or video-sharing platform. In addition, the potential impact that the system, or the age verification systems implemented, may have on use by users with disabilities should be assessed, for example, by ensuring that screen readers can be used to successfully complete the verification process.
- More age assurance solutions should be made available, allowing users to choose which one to use according to their characteristics and needs.
- Age verification shall not require the creation of a user account for the service offered by the regulated entity. In addition, proof of age cannot be stored in a user account on that service. In any case, the age verification obligation applies to each access, with or without a user account.

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

- Non-discrimination is one of the four general principles of the UNCRC. Differences between children in terms of language, skills, socio-economic status, etc. should be taken into account during the age assurance process.
- This criterion refers to the ability of the age assurance system to avoid or minimise unintended bias and discriminatory outcomes towards users. Therefore, where applicable, regulated entities must ensure that age verification mechanisms have been trained on different datasets, in order to avoid discriminatory results for certain user groups, for example a lower degree of technical precision for users of a given ethnicity when the mechanism is based on facial age estimation, or also to prevent underage users from being mistakenly identified as adult users, or adult users from being mistakenly identified as minors.



viii. **Transparency:**

- Regulated entities should be transparent towards users regarding the systems and data processed and the purposes, through simple, clear, and complete explanations, not only for adults but also for minors.
- Regulated entities shall make available on their websites data on the accuracy and effectiveness of the age assurance systems used, reporting the metrics and parameters employed in the evaluation as well as the results obtained.

ix. **Training and information:**

- The Authority considers it important to inform and raise awareness among minors, parents, educational staff, and youth worker about good IT practices and Internet-related risks. Activities relating to the implementation of Parental Control have highlighted the importance of this aspect.

x. **Complaints handling:**

- The age assurance service provider must provide at least one channel to receive and handle complaints in a timely manner in case of incorrect age decisions.

xi. **Monitoring:**

- The Authority reserves the right to periodically verify and evaluate the effectiveness of the technical and organisational measures referred to in these technical specifications, aimed at mitigating security and personal data protection risks.

### **Article 3**

#### **SCOPE**

These technical specifications are established in implementation of Article 13b(3) of Decree-Law 123/2023 as converted into Law No 159 of 13 November 2023, which concerns services that disseminate pornographic content through video-sharing platforms and websites, and, therefore, entities that disseminate or publish pornographic content.

In this regard, with Decision No 88 of 8 February 2024, the Data Protection Commissioner, having examined the draft measure previously sent by the Authority, gave a favourable opinion on the launch of the public consultation; Comments were also

made by way of institutional cooperation, which the Authority considered appropriate to take into account in the final version of the text submitted for public consultation.

Among the comments, there is also the observation that the legislation in force — also specifically referring to the role of the Authority — repeatedly refers to the need to implement age verification mechanisms, establishing that minors have the right to a higher level of protection from content that may impair their physical, mental, or moral development, including by introducing stricter measures against any information society service.

It notes, in this regard, that the European Commission supports and promotes the implementation of rules aimed at the protection of minors online and Article 28 of the DSA requires that all online platform providers accessible to minors 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. In addition, it is noted that, in accordance with Article 35(1)(j) of the DSA, providers of very large online platforms and very large online search engines shall adopt systemic risk mitigation measures, including ‘targeted measures to protect the rights of the child, including age verification and parental control tools, tools aimed at helping minors signal abuse or obtain support, as appropriate’.

The provisions of Article 8 of the GDPR must also be taken into account.

They also note the powers specifically conferred on the Authority by Articles 41 and 42 of the TUSMA, such as, in particular, Article 41(7), which provides that:

*7. Without prejudice to Articles 14 to 17 of Legislative Decree No 70 of 9 April 2003, and without prejudice to the provisions of the preceding paragraphs, **the free circulation of programmes, user-generated videos and audiovisual commercial communications conveyed by a video-sharing platform whose supplier is established in another Member State and directed to the Italian public may be restricted, by decision of the Authority, in accordance with the procedure laid down in Article 5(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(1).***

In addition, Article 42(1) and (6) provide that:

*1. Without prejudice to Articles 14 to 17 of Legislative Decree No 70 of 9 April 2003, providers of video-sharing platforms under Italian jurisdiction **must take appropriate measures to protect:***

*a) **minors from programmes, user-generated videos, and audiovisual commercial communications that may harm their physical, mental, or moral development in accordance with Article 38(3);***

*[omitted]*

*6. For the purposes of protecting minors referred to in paragraph 1(a), **the most harmful content shall be subject to the strictest access control measures.***

Under Article 42(7) of the TUSMA:

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

*[omitted]*

***f) establish 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 harm the physical, mental or moral development of minors;***

*[omitted]*

***h) establish parental control systems under the supervision of the end-user as regards content that may impair the physical, mental, or moral development of minors;***

This regulatory framework also influences this document, which, in various parts, makes broader references to the need for the protection of minors, such as:

- vi 'Functionality, user-friendliness and non-obstructive access to content on the internet' where it is specified that 'age guarantee systems must be user-friendly and based on the abilities and characteristics of minors. Age verification should not restrict access to the internet but rather facilitate it by not creating unnecessary obstacles to the use of services and content';
- vii 'inclusivity and non-discrimination' where it is specified that 'differences between children in terms of language, skills, socio-economic status, etc. should be taken into account during the age assurance process';
- ix 'Training and information' where it is specified that the Authority considers it important to inform and raise awareness among minors, parents, educational staff, and youth worker about good IT practices and Internet-related risks.

The Authority considers, in light of the regulatory framework referred to above and the comments made by participants during the consultation, that the technical and procedural arrangements for verifying the age of majority of users adopted by this measure are highly recommended, as they are effective, suitable, proportional, and functional, for their own use as well as by entities other than those directly regulated herein and with reference to other types of content, in addition to those of a pornographic nature, which could in any case harm the physical, mental, or moral development of minors, such as the categories provided for by Resolution 9/23/CONS.

## **Annex B to Resolution No /24/CONS**

### **EUROPEAN AND NATIONAL FRAMEWORK ON TECHNICAL AND PROCEDURAL ARRANGEMENTS FOR ASCERTAINING THE AGE OF MAJORITY OF USERS**

#### **Summary**

<b>I. Premise.....</b>	<b>25</b>
<b>II. National regulatory framework.....</b>	<b>33</b>
<b>III. Interventions at European level.....</b>	<b>36</b>
<b>The Task Force on Age Verification.....</b>	<b>40</b>
<b>IV. Standardisation and regulatory initiatives.....</b>	<b>48</b>
<b>ANNEX 1.....</b>	<b>49</b>
<b>I. Standardisation and regulatory initiatives.....</b>	<b>49</b>
<b>I.1 The euConsent project.....</b>	<b>49</b>
<b>I.2 The public consultation by the UK regulator Ofcom.....</b>	<b>55</b>
<b>I.3 The CNIL's position in France on the balance between the protection of minors and respect for privacy.....</b>	<b>61</b>
<b>I.4 The public consultation by the French regulator Arcom.....</b>	<b>69</b>
<b>I.4 The public consultation by the Spanish regulator.....</b>	<b>76</b>
<b>I.5 German regulation.....</b>	<b>82</b>
<b>I.6 The public consultation by the Irish regulator.....</b>	<b>85</b>
<b>I.7 The Spanish Data Protection Agency (AEPD) – age verification.....</b>	<b>88</b>
<b>I.8 Observations on the use of public systems.....</b>	<b>95</b>

## I. Premise

### Online age verification methods for minors

For more than two decades, a limited range of age verification methods have been available online to protect minors from accessing online content that is not suitable for their age. However, the protection of that group of users in the context of online activities is becoming an increasingly vital aspect in the current social context.

As noted in the report '*On line age verification methods for children*', drawn up by the EPRS (*European Parliamentary Research Service*), in February 2023, several countries were introducing laws and/or codes of conduct to address this issue. Efforts are also being intensified at EU level through the adoption of a code of conduct, which is being analysed. The identification of user age verification measures presents, as further clarified below, several elements of complexity, not least in the area of privacy protection, monitoring, and the need to improve the digital skills of parents and children.

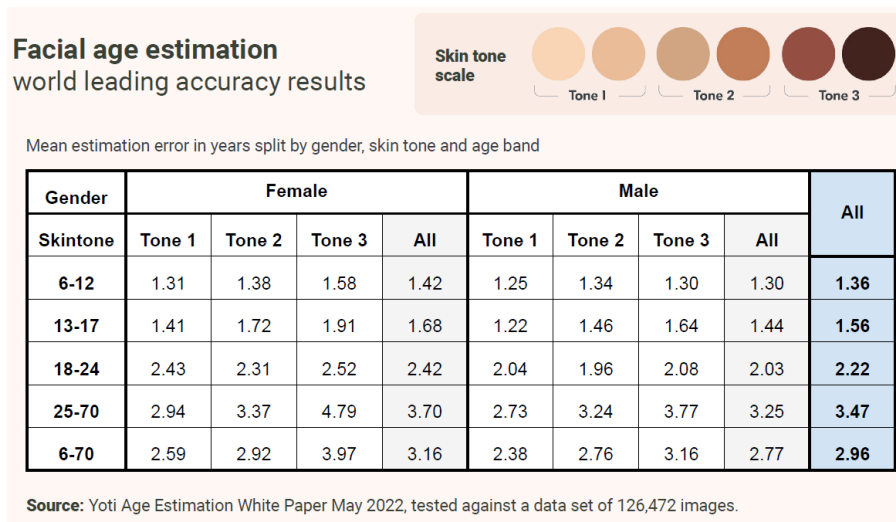
On the basis of the above-mentioned document, it is noted that, also as a result of the coronavirus pandemic, children have become accustomed to spending more time online. Global estimates reveal that one in every three children is an Internet user and that one in every three Internet users is under the age of 18. In the EU, most children 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 (e.g. in some cases, social media require a minimum age of 13 years for their users). Overall, it is noted that digital services do not use adequate methods of age verification or parental consent.

Online age verification methods are increasingly diversified. Below is a list of those that, according to the EPRS report, are considered to be the most common.

- 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. Popular examples include the self-declaration of one's date of birth.
- B. Credit card:** here users are required to have their cards checked for validity, 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 the age of majority. 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, the document in question states that it is not possible to ascertain that the person using the card is the legitimate holder; in addition, the age for owning a credit card varies from country to country.

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

Some providers consider it to be an instantaneous process — one that is scalable to tens of millions of units per day — where no image is stored. Below is a table containing, based on analyses conducted by certain analysts, an indication of the performance in terms of the statistical error of the estimate.



**D. Analysis of online usage patterns (analysis of online behaviour):** these are age verification systems by inference, such as by importing an individual's internet browsing history or analysing their 'maturity' through a questionnaire or user-generated content or online purchases.

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

**F. Online verification:** this is carried out by means of document checks. For example, in the case of Photo-ID matching, the photograph on the identity document uploaded by the user, which also includes the date of birth, is compared with a photographic image of the user taken at the time of uploading the document to verify whether it is the same person.

**G. Parental consent:** some apps and services require parental consent to register a minor with a digital service. However, parental authority is rarely fully verified.



Demonstrating parental authority/guardianship could 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 the tools offered 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 needed to access online services, share digital documents, or simply demonstrate a specific personal attribute, such as age, without disclosing full personal details or other personal data. Within the EU, there is a proposal to create a European Digital Identity Wallet<sup>6</sup>.
- K. **Age verification via a specific app:** these are applications that are, for the most part, 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 take a biometric selfie to create their own reusable digital ID. Once verified, access takes place by scanning a QR code.
- L. To the above list, one can add models that are based on **the mobile phone number** and comparison with the data held by the phone operator. Others carry out verification by means of **e-mail** or even by means of **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 years of age is shared with the site/service provider requesting verification of the user's age. Your personal data, including your date of birth, is not shared with the website/service provider.

Only recently, according to the research carried out, have social platforms started to apply age verification measures.

- A. In 2022, **Instagram** started testing a tool to ensure that users are the age they claim to be; in some cases, it has also started 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 parent-approved contacts.
- D. **TikTok** does not have an age verification method but may prohibit accounts after registration.

---

<sup>6</sup> <https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-toolbox>

- E. **Twitter** verifies parental consent by requesting documentation (identity card/birth certificate, etc.). Twitter says the 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.

According to the conclusions of the aforementioned report, some 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 these pose risks to privacy and cybersecurity. Given the sensitivity of the data collected by some age verification systems, **some suggest implementing a certification provided by third parties**. To date, there are no common EU guidelines on methods for determining age verification, and it has been found that minors easily bypass most solutions.
- B. Content not sufficiently appealing to minors: As apps and digital services for minors tend to provide a limited set of features, many prefer to lie about their age 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, within the EU, the following framework is presented.

Before the adoption of the General Data Protection Regulation (**GDPR**), which entered into force in 2018, there were no specific restrictions on the online processing of children's data in Europe. The GDPR introduces, in Article 8, verification by data controllers with regard to age and parental consent. Furthermore, recital (38) specifies that minors deserve specific protection in relation 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. This specific protection should, in particular, concern the use of a minors' personal data for marketing purposes or the creation of personality or user profiles and the collection of personal data relating to minors when using services provided directly to a minor. The **Audiovisual Media Services Directive (AVMSD)** requires the adoption of appropriate measures to protect minors 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-appropriate 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 proposal on eID**, the **Commission intends to strengthen age verification methods through a robust certification and interoperability framework**. In addition, the **Proposal for a Regulation to combat online child sexual abuse** provides for better online age verification. The **euCONSENT project**, co-funded by the EU, which is developing an interoperable browser-based age verification method, should also be mentioned. The European Parliament has on several occasions called for better age verification methods to protect children online, including in its own-initiative report on consumer protection in online video games adopted in January 2023 and in its resolution of March 2021 on children's rights in light of *the EU Strategy on the Rights of the Child*. Similarly, better age verification methods to protect children 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 Trusted, 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, drafted by **ERGA Subgroup 1**.

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

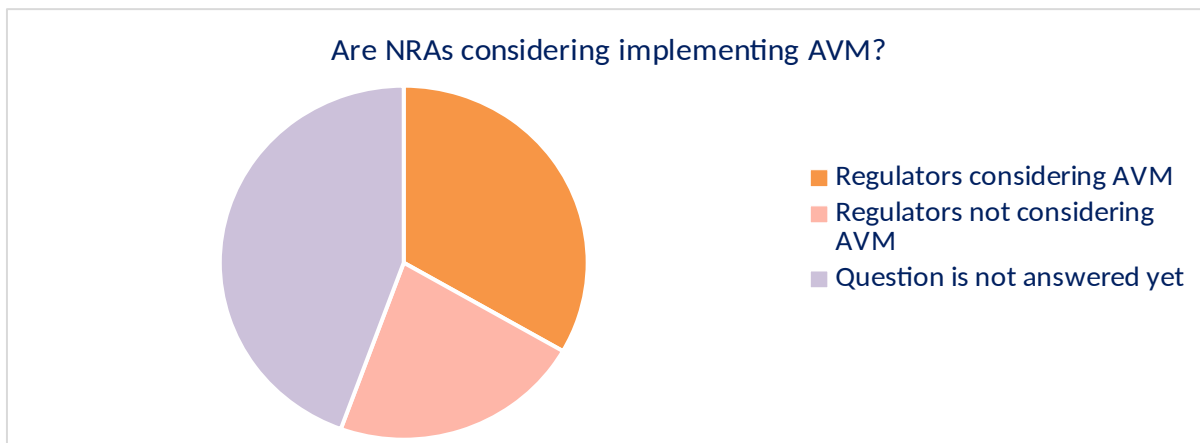
ERGA also recognises that identifying and implementing efficient mechanisms to prevent children from accessing harmful content, and in particular pornographic content, raises a number of challenges, both in terms of efficiency (as some of these mechanisms can be easily circumvented) and of privacy. The 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 broad implementation by all relevant actors.

In order to collect data in this regard, a questionnaire was sent to the countries participating in ERGA on 17 July 2023 concerning the transposition of Articles 6(a) and 28b(3)(f) of the AVMS Directive and the national implementation of the AVMS, with particular attention to access to pornographic material by minors. 27 NRAs responded on behalf of 25 EU Member States and one EFTA Member State.

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

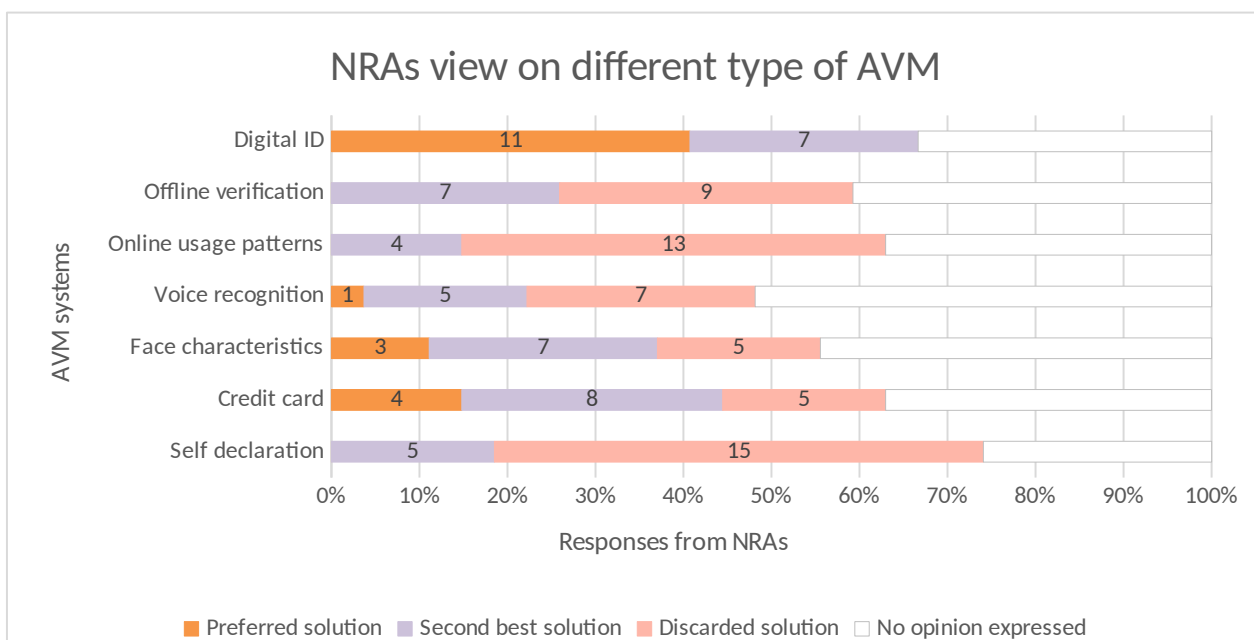
**Particularly in light of the implementation of age verification mechanisms in ERGA member states to restrict minors' access to pornographic content**, 12 NRAs replied that they did not yet have a specific position.

9 NRAs replied that the AVM was taken into account, while 6 NRAs replied to the contrary.



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

As regards the technical solution, the following picture emerges in response to the question of which is the **ERGA members' preferred solution for AVM**:



**Age verification based on a digital identity**, such as the use of tools offered by the State to verify the identity of persons in general, **seems to be the preferred solution**<sup>7</sup>.

**On the contrary, self-declaration is the least preferred solution** among those proposed based on the responses, as 15 NRAs rejected it, 5 NRAs placed it at the second-best level, and none as the preferred solution.

The models of **online use and offline verification** are also considered inadequate and no NRA mentions them as the preferred solution<sup>8</sup>.

As regards **credit card-based AVM**, 4 NRAs responded in favour, 5 NRAs were against, and 8 NRAs were not against but still had concerns in this respect.

Poor consensus may be seen with regard to methods based on the analysis of facial features or voice recognition<sup>9</sup>.

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 safety of the various systems. Intervention by an independent intermediary is an option considered by many NRAs, demonstrating concerns related to privacy. In this regard, the solution based **on a digital identity** seems to be preferred by most NRAs, although some are not entirely convinced of it. **Self-declaration is almost unanimously rejected** as an effective AVM.

### Technical solutions available on the market

The systems created by third parties, which provide the age verification service to applicants, allow the following information to be obtained:

- whether the user's age is above the minimum requirement;

<sup>7</sup> 11 NRAs (BE – VRM, BE – CSA, DE, EE, HR, LT, LU, LV, NL, SI, SK) classified it as the preferred solution, 7 NRAs (AT, CZ, EL, FR, IT, PL, PT) as the second favourite solution and no NRAs responded by rejecting the solution.

<sup>8</sup> The online use models received 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 received 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.

<sup>9</sup> the first received 3 responses (AT, DE, NL) in favour, 7 responses (HR, FR, IT, LV, LU, PL, SK) as second-best, and 5 responses (BE – VRM, BE – CSA, CZ, EE, LT) against; the second received 1 response (NL) in favour, 5 responses (AT, IT, LU, LV, SK) as second-best, and 7 responses (BE – VRM, BE – CSA, CZ, EE, HR, LT, PL) against.

- the age of the user.

In general, various methodologies are used, among which the most common are the following:

1. [Age estimation using facial recognition \(biometrics\)](#)
2. [Scanning of an identity document](#)
3. App
4. [Credit card](#)
5. [Mobile number](#)
6. [Matching 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 and one will be analysed by the age estimation system based on Artificial Intelligence algorithms.

### **2. Scanning of an identity document**

The user is asked to scan the identity document using the camera on their device. The provider extracts the information from the identity document and verifies whether the age is greater than that required by the organisation 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 identity document belongs to the user. The acquired data, such as the identity document and the selfie, are stored in the data centre. Once the session is completed, all personal information is deleted.

### **3. App**

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

### **4. Credit card**

The user is asked to enter the number, expiry date, post code, and CV2 number of the credit card.

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

### **5. Mobile number**

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



This data is sent to the operator. Users will receive an SMS 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 phone service provider then confirms that the data entered on the site corresponds to the mobile service account data, which are 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 civil registry certification body to confirm that it is accurate and to obtain or confirm your date of birth.

## Reusable age controls

To minimise the number of times online age verification is required, some providers develop an ‘age token’ system. Age tokens function as digital evidence of an age check and allow the result of the age check to be reused for as long as the organisation allows. You can save age tokens in an ‘age account’. This allows you to access the organisation’s website, on another browser or another device without having to prove your age each time<sup>10</sup>.

## II. National regulatory framework

The Italian legal system has addressed several provisions governing the age of recipients of the services offered by online platforms.

Legislative Decree No 208 of 8 November 2021 on the ‘Implementation of Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 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 (Audiovisual Media Services Directive) in view of changing market realities’, (hereinafter referred to as TUSMA), as amended by Legislative Decree No 50 of 25 March 2024, introduced into Italian law, in Article 3(1)(c), 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 objective of the service, a distinguishable section or essential functionality thereof is the provision of programs or user-generated videos, addressed to the general public, over which the video-sharing platform provider has no editorial responsibility, for the purpose of informing, entertaining, or educating through electronic

---

<sup>10</sup> When you visit a website that uses age tokens, clicking on a button to verify your age through the provider will present you with the option to access the age account. You will be asked to enter your username and password. The website checks whether there are any age tokens in the user’s browser that match the criteria defined by the company linked to the user’s account. If yes, the provider returns a result to confirm that a previous check has already been carried out and whether your age token meets the above criteria.

communications networks within the meaning of [Article 2\(a\) of Directive 2002/21/EC of the European Parliament and of the Council of 12 July 2002](#), and whose organisation is determined by the provider of the video-sharing platform, including by automated means or algorithms, in particular by displaying, 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 the providers of those services established or deemed to be established in Italy.

In addition, that provision introduced into Italian law a specific provision aimed at providers of such services that are established in another Member State and whose content disseminated there is aimed at the Italian public.

In this regard, Article 41(7) provides that:

*Without prejudice to Articles 14 to 17 of Legislative Decree No 70 of 9 April 2003, and without prejudice to the provisions of the preceding paragraphs, the free circulation of programmes, user-generated videos and audiovisual commercial communications conveyed by a video-sharing platform **whose supplier is established in another Member State and directed to the Italian public may be restricted**, by decision of the Authority, in accordance with the procedure laid down in Article 5(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(1);*

Pursuant to Article 42(1) and (6) of the same TUSMA, it is also provided that:

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

*[omitted]*

6. *For the purposes of protecting minors referred to in paragraph 1(a), the most harmful content shall be subject to the strictest access control measures.*

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

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

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

[omitted]

f) establish 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 harm the physical, mental or moral development of minors;

[omitted]

h) establish parental control systems under the supervision of the end-user as regards content that may impair the physical, mental, or moral development of minors;

Finally, Decree-Law No 123 of 15 September 2023, converted with amendments into Law No 159 of 13 November 2023, introduced ‘Urgent measures to combat youth hardship, educational poverty and child crime, as well as child safety in the digital environment’ (hereinafter Decree).

In particular, Article 13a, entitled ‘Provision for the verification of the age of majority for access to pornographic sites’, establishes that:

1. The access of minors to pornographic content is prohibited, as it undermines respect for their dignity and compromises their physical and mental well-being, constituting a public health issue.
2. Without prejudice to the provisions of Article 42 of Legislative Decree No 208 of 8 November 2021, website operators and providers of video-sharing platforms which disseminate pornographic images and videos in Italy, are required to verify the age of majority of users, in order to prevent access to pornographic content by minors under the age of eighteen.
3. The Communications Regulatory Authority shall, within 60 days of the date of entry into force of the law converting this Decree, by adopting its own measure, after consulting the Data Protection Commissioner, lay down **the technical and procedural arrangements** that the entities referred to in paragraph 2 are required to adopt for the verification of the age of majority of users, ensuring a level of security appropriate to the risk and respect for the minimisation of personal data collected due to the purpose.
4. Within 6 months of the date of publication of the measure referred to in paragraph 3, the persons referred to in paragraph 2 shall have in place effective age verification systems that comply with the requirements set out in the aforementioned measure.
5. The Communications Regulatory Authority shall ensure the correct application of this Article and, in the event of non-compliance, shall inform the entities referred to in paragraph 2, including ex officio, of the infringement, applying the provisions of Article 1(31) of Legislative Decree No 249 of 31 July 1997, and shall warn them to comply within 20 days. In the event of non-compliance with the warning, the Communications Regulatory Authority shall take all appropriate measures to block the site or platform until the parties referred to in

*paragraph 2 have restore conditions of service provision that comply with the contents of the Authority's warning.*

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

In light of the legislative framework set out above, and with a view to making it effective, the Authority, in the context of its institutional tasks, has launched, by means of Resolution No 9/24/CONS, a procedure involving all the parties concerned in various capacities, with a view to adopting a measure laying down the technical and procedural modalities that the parties referred to in Article 13a(2) of the *Decree* are required to adopt for the verification of the age of majority of users, ensuring a level of security appropriate to the risk and compliance with the minimization of personal data collected due to the purpose.

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

In accordance with Article 3 of the resolution, the Authority must, following the consultation, obtain the opinion of the Data Protection Commissioner.

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

### **III. Interventions at European level**

At European level, there have been various regulatory provisions to protect minors from content disseminated on online digital platforms that may harm their moral, physical, and psychological development.

In particular, Directive (EU) 2018/1808 of 14 November 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 (Audiovisual Media Services Directive) added point (aa) to Article 1 of Directive 2010/13/EU, 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 principal purpose of the service or of a dissociable section thereof or an essential functionality of the service is devoted to providing programmes, user-generated videos, or both, to the general public, for which the video-sharing platform provider does not have editorial responsibility, in order to inform, entertain or educate, by means of electronic communications networks within the meaning of point (a) of Article 2 of Directive 2002/21/EC and the organisation of which*

*is determined by the video-sharing platform provider, including by automatic means or algorithms in particular by displaying, tagging and sequencing’.*

In addition, recital (45) of the aforementioned Directive states that ‘*There are new challenges, in particular in connection with video-sharing platforms, on which users, particularly minors, increasingly consume audiovisual content. In this context, harmful content and hate speech provided on video-sharing platform services have increasingly given rise to concern. In order to protect minors and the general public from such content, it is necessary to set out proportionate rules on those matters’.*

In addition, the aforementioned Directive then also notes in recital 47 that ‘*A significant share of the content provided on video-sharing platform services is not under the editorial responsibility of the video-sharing platform provider. However, those providers typically determine the organisation of the content, namely programmes, user-generated videos and audiovisual commercial communications, including by automatic means or algorithms. Therefore, those providers should 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 contains incitement to violence or hatred directed 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 the dissemination of which constitutes a criminal offence under Union law’.*

The aforementioned Directive introduced Article 28b 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 programmes, user-generated videos and audiovisual commercial communications which may impair their physical, mental or moral development in accordance with Article 6a(1)’.*

Finally, Article 28b(3) provides that Member States are to ensure that all video-sharing platform providers under their jurisdiction apply appropriate measures for the protection of their users, determined in light of the nature of the content concerned, the harm it may cause, and that they are practical and proportionate; in particular, with regard to the protection of minors, it provided that the most harmful content disseminated on a video-sharing platform shall be subject to the strictest access control measures. To this end, it provided in point (f) that such measures consist, as the case may be, of the activities of ‘*establishing and operating age verification systems for users of video-sharing platforms with respect to content which may impair the physical, mental or moral development of minors’.*

The recent Regulation (EU) 2022/2065 of 19 October 2022 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Act or DSA) defined, in Article 1(1)(i), online platforms as follows: ‘*a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public,*

*unless that activity is a minor and purely ancillary feature of another service or a minor functionality of the principal service and, for objective and technical reasons, cannot be used without that other service, and the integration of the feature or functionality into the other service is not a means to circumvent the applicability of this Regulation’;*

With this regulation, the European Commission addressed the issue, supporting and promoting the implementation of rules aimed at the protection of minors online. In particular, Article 28 of the Digital Service Act requires that all online platform providers accessible to minors 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 clarified below.

In particular, Article 35 of the Regulation provides that providers of very large online platforms and very large online search engines should take reasonable, proportionate, and effective mitigation measures adapted to the specific systemic risks identified pursuant to 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: *‘taking targeted measures to protect the rights of the child, including age verification and parental control tools, tools aimed at helping minors signal abuse or obtain support, as appropriate’*.

Adoption of the eIDAS Regulation<sup>11</sup> in 2014 enabled Member States to use national electronic identification schemes (eIDs) to access online public services across borders. As the digital landscape evolves, 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 evident 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 possibility 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 across the EU, moving seamlessly across borders without ever losing control of their data, with privacy and security at the heart of the project. The wallets supports the principles outlined in the EU Declaration on Digital Rights and Principles<sup>12</sup> and contributes to reaching the objective of the Digital Decade Policy Programme<sup>13</sup> to ensure that 100% of EU citizens have access to a digital identity by 2030.

In **April 2024**, the European Council definitively approved the proposal to amend the Regulation on the establishment of a new framework for a European Digital

---

<sup>11</sup> Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS)

<sup>12</sup> <https://digital-strategy.ec.europa.eu/en/policies/digital-principles>

<sup>13</sup> [https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030\\_en](https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en)



Identity<sup>14</sup>. The aim is to have a digital identity system recognised throughout Europe, regardless of the Member State in which it is made available (a harmonised digital identity framework).

The Regulation **requires Member States to issue a European Digital Identity Wallet**<sup>15</sup> within the framework of an electronic identification scheme **in line with common technical standards**, following a mandatory conformity assessment and voluntary certification in the context of the European cybersecurity certification framework, as set out in the Cybersecurity Regulation<sup>16</sup>. The provisions aim to ensure that natural and legal persons have the possibility to securely request and obtain, store, combine and use personal identification data, attributes and electronic attestations of attributes for online and offline authentication, as well as to access online public and private goods and services, with full user control.

Among the reasons behind the Regulation is the fact that currently, in most cases, citizens cannot digitally exchange across borders, securely and with a high level of data protection, information relating to their identity such as addresses, age, professional qualifications, driving licences, other permits, and payment data. Therefore, the EUDI wallet would make it possible to overcome those limits by offering the possibility to exchange minimum identity attributes necessary to access certain online services for which authentication is required, such as proof of age. In addition, the new eIDAS Regulation provides that, **where very large online platforms, as defined by the DSA, require user authentication in order to access online services, they must also accept the use of European Digital Identity Wallets, strictly at the voluntary request of the user, including with regard to the minimum attributes necessary for the specific online service for which authentication is required, such as proof of age**<sup>17</sup>.

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

**By 2026, each Member State shall make a digital identity wallet available to citizens and shall accept European Digital Identity Wallets from other Member States.**

---

<sup>14</sup> [Regulation 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation \(EU\) No 910/2014 as regards establishing the European Digital Identity Framework.](#)

<sup>15</sup> The European Digital Identity Wallet is defined as a product or service that allows the user to store identity data, credentials and attributes linked to his or her identity, provide them to relying parties on request 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.

<sup>16</sup> It consists of a set of technologies, processes and protective measures designed to minimise the risk of cyber attacks.

<sup>17</sup> Paragraph 3 of Article 12b introduced by the eIDAS 2.0 Regulation



### 1.1 *The Task Force on Age Verification*

On 23 January 2024, the work of the *Task Force on Age Verification* commenced with the presentation, by the Commission, of a number of studies carried out by experts in the field.

First, some definitions were provided, as mentioned below.

**Age assurance** is the generic term for methods used to determine an individual's age or age group at varying 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 ticks a box to declare that they are over/under a certain age.

**Age estimation** consists of methods that determine that a user is likely to be of a certain age, of a certain age group, or above or below a certain age. Age estimation methods include automated analysis of behavioural and environmental data, comparing how a user interacts with a device or other users of the same age, and metrics derived from analysis of movements or testing of their skills or knowledge.

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

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

In this context, the *Task Force on Age Verification* shall discuss and support the development of a European age verification framework and approach, as well as ensure coherence and a common approach across the EU.

A study presented by the experts contracted by the Commission summarises the age verification methodologies identified:

- **Self-declaration:** Users declare their age/age group without providing any other evidence.
- **Rigid identifiers:** Users provide verified identity documents (e.g. a passport) to prove their age.
- **Credit cards:** use of credit card information to verify that a user is over 18 years of age.
- **Blockchain-based identity:** use of decentralised technologies such as the blockchain to create users' digital identities, and to use such identities for Age Verification.

- **Account holder confirmation:** verification based on confirmation from an existing verified account holder that another user is of the required age to use the platform.
- **Cross-platform authentication:** using existing user accounts with large platforms (e.g. Google, Apple, etc.) to authenticate a user's age for other products/services.
- **Facial estimation:** use of artificial intelligence to analyse a person's facial features in order to estimate their age.
- **Behavioural profiling:** use of artificial intelligence to analyse users' online activity to estimate their age.
- **Ability test:** testing the user's ability or aptitude in order to estimate their age.
- **Third-party age assurance services:** use of third-party companies for age assurance services. Third parties may use any of the other methods for age assurance.

The requirements identified in the study are as follows:

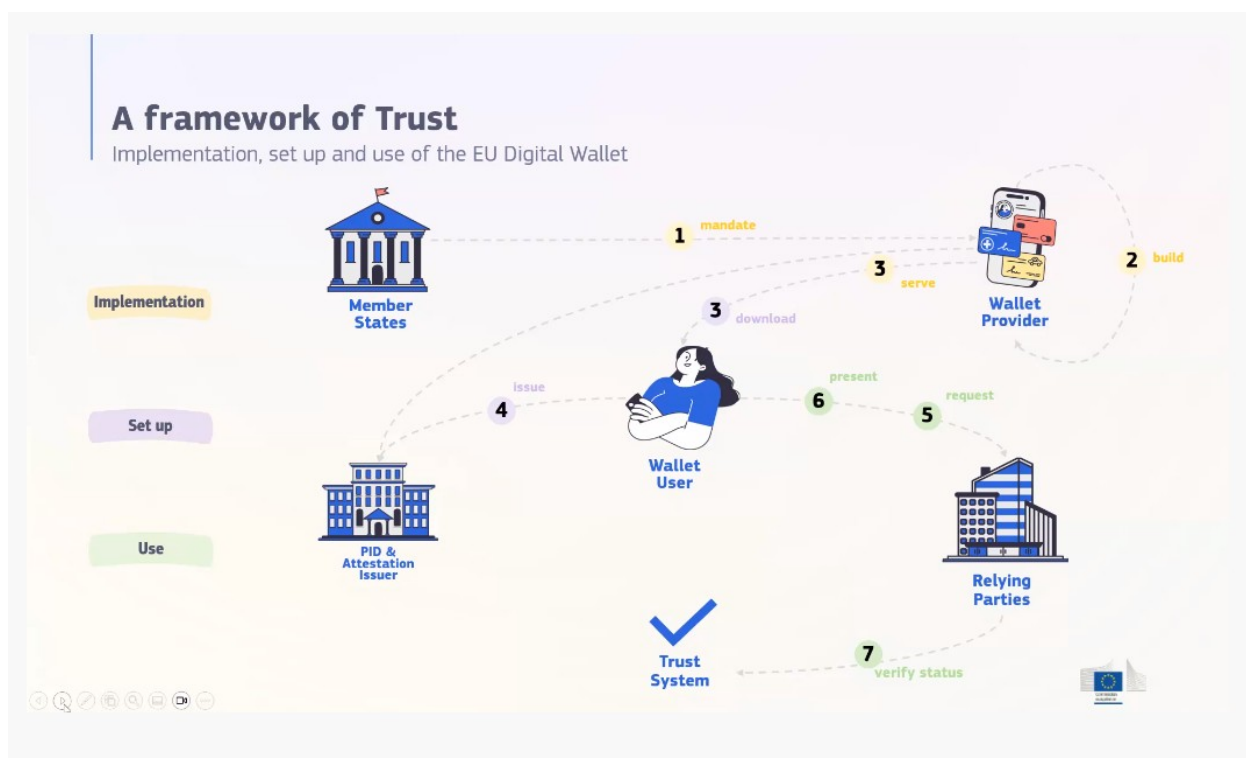
- i. **Proportionality and subsidiarity:**
  - A general requirement that can play a role in respecting other requirements.
  - Balance between the means used to achieve the intended objective and its impact on the limitation of the rights of individuals.
  - Use of the least invasive tool to achieve the set objective.
- ii. **Privacy:**
  - It is necessary to follow the data protection principles established by the GDPR (data minimisation, accuracy, storage limitation, etc.).
  - High level of protection of the privacy of minors (OSA).
  - Age assurance may conflict with privacy rights.
- iii. **Security:**
  - Sufficient IT security measures need to be implemented (GDPR, proposal for a CRA).
  - The sophistication of cyber attacks 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.
  - The functionality can encourage adoption by users.
  - However, the functionality could dilute effectiveness.
- vi. **Inclusivity and non-discrimination:**
- Non-discrimination is one of the four general principles of the UNCRC.
  - Differences between children in terms of language, skills, socio-economic status, etc. should be taken into account during age assurance.
  - Age assurance could lead to discrimination and exclusion in a number of ways.
- vi. **Promoting participation and access:**
- Age verification should not amount to erroneously blocking children or providing them with inferior services.
  - Digital technologies empower children and age assurance should not be an obstacle to this, but rather promote it.
- viii. **Transparency and accountability:**
- Age assurance providers should be transparent with users regarding the age assurance used, and age assurance should be understandable to children.
  - Platforms must be responsible for implementing age assurance.
- viii. **Notification, dispute and redress mechanisms:**
- Due process should be followed for age assurance decisions.
  - There must be channels of communication to notify, dispute and seek redress against wrong Assurance decisions.
- viii. **Listening to the views of minors:**
- According to the UNCRC, children have the right to be heard.
  - Platforms should engage with and pay attention to children's views on age assurance.

As part of the work on 18 March 2024, representatives of the European Commission presented the project for the implementation of the EUDI wallet<sup>18</sup> 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's APP to securely obtain, store and share important digital documents and will have the opportunity to easily prove who they are when accessing online digital services.

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

The process envisaged by the Commission for the implementation, setting up and use of the EUDI wallet follows the scheme set out below.



Initially, Member States mandate (step 1 and step 2) providers (*wallet providers*) to implement digital identity wallets in compliance with the framework laid down by the Regulation, for example by developing an APP wallet that can be downloaded by users on their mobile devices.

<sup>18</sup> <https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/>

Through the digital identity wallet APP, the user will be able to store and manage his or her digital identity, as well as any attributes (e.g. age, nationality, gender, etc.) and attestations (e.g. proof of age, driving licence, study certificates, etc.) validated by appropriate issuers (*PID & Attestation issuer*, step 3 and step 4) that interact with the digital wallet providers. Users will then be able to use the digital identity wallet to identify and authenticate themselves online when requested to do so by public/private entities in order to access their services (*relying parties*, step 6 and 5).

As regards age verification through the Digital Identity Wallet, the Commission described **the key requirements underpinning the project**:

- Provide proof of age (+18) online when requested to do so by a service provider/platform;
- **The proof of age must not disclose any personal information of 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;**

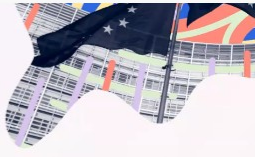

As regards age verification mechanisms, the Commission has proposed four process scenarios that shall be made available to users using the EUDI wallet. **The assumptions of the project are to keep the user's identity hidden when a proof of age is requested, and to ensure that any third parties involved in the age verification process are not aware of the use the user will make of the certification.**

The first scenario (*Age Disclosure – over 18 attribute*) consists of the possibility for the user to share the attribute “of majority age” based on the 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*) provides for the creation of a pseudonymous attestation by the user directly within the digital wallet, which includes only the information of the user's ‘age of majority’. This attestation may be sent to the provider requesting proof of age.

The third scenario (*Attestation issued by a trusted 3rd party*) provides for the generation of a pseudonymous attestation by a certified third party, which contains only the information of the user's age of majority.

## Age Verification – Current Wallet Implementation Options

- 1 Age Disclosure (“over 18” attribute)**

User shares the “age over 18” attribute from the basic identity data already included in the wallet without sharing any other data (selective disclosure).


  - **No Cost and existing wallet functionality (+), trust with identity data provider (+), profiling possible (-)**
- 2 Self-Attestation created by the user**

User creates a pseudonymous attestation within the Wallet only with proof of age (“over 18 attribute”)

  - **Low Cost and simple implementation (+), risk of data manipulation, trust with user - no third trusted party (-), profiling difficult (+)**
- 3 Attestation issued by a trusted party**



A trusted 3rd party **issues** a pseudonymous attestation only with the age information

  - **Cost to be covered by user, provider, or public and implementation effort (-), trust with third party (+), profiling difficult (+)**



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

## Age Verification – Future Wallet Implementation Option





- 4 Age Disclosure using Zero Knowledge Proof Protocols (“Option 1+”)**

User shares the “age over 18” attribute from the basic identity data already included in the wallet without sharing any other data (selective disclosure). **The attribute uses Zero-Knowledge Technology which makes profiling impossible.**

A zero-knowledge proof is a cryptographic method by which one party can prove to another party that a given statement is true without providing any other information. Zero-knowledge proof protocols are not yet technically mature, only a limited number of implementations are available.

  - **Low cost as self-attestation (+), Trust with identity data provider (+), Strong protection against profiling (+)**



The Commission has produced a pilot version of the digital wallet which will be subject to a first phase of testing with the voluntary involvement of Member States. During this phase (which is the *POC - Proof of Concept*), any comments and

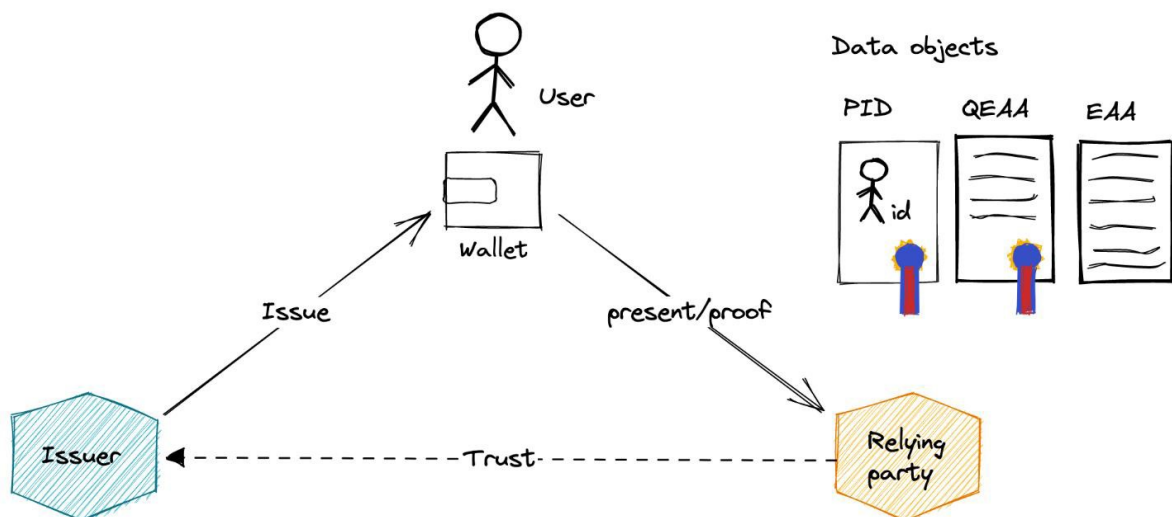


suggestions from Member States on the age verification mechanisms implemented through the wallet will be taken into account.

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

As part of its work on 23 April 2024, intended to kick-start 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 that interact in the request, certification and verification process, i.e. the user using the digital wallet, the issuer who provides the proof of age and the relying party to whom the user submits the proof of age.



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

1. **PID (Personal Identification):** a set of data issued in accordance with Union regulations or national laws and which makes it possible to establish the identity of a natural person. The PID includes both mandatory information (name, short name, date of birth) and optional information ('age in years, surname of birth, address of residence, country of residence, nationality').
2. **EAA (electronic attestation of attributes):** consists of an attestation in electronic format that allows the authentication of particular attributes<sup>19</sup> (e.g. 'age of majority');

<sup>19</sup> 'Attribute' is defined as a prerogative, characteristic or quality of a natural or legal person or entity, in electronic form



3. **QEAA (qualified electronic attestation of attributes):** attestation in electronic format issued by a qualified trust service provider, such as a driving license, age of majority, etc.

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

- **Scenario 1 - age disclosure (attribute ‘age over 18’)**

The user shares the ‘age over 18’ attribute from the basic identity data already included in the wallet without sharing any other data (selective disclosure). In this case, the website/platform requires the user to verify their age by providing them with a QR CODE. By scanning the QR CODE using the digital wallet app, the user receives a request to present the information contained in the PID (e.g. the ‘age of majority’ attribute) and consents to share the requested information. The website/platform thus receives information on the age of majority from the digital wallet.

- **Scenario 2 - attestation (pseudonym) issued by a trusted entity**

A trusted third party issues a pseudonymous attestation<sup>20</sup> that only contains information about the age. In this case, the user requests a certifying body to issue a certified attestation of majority. The certifying body shall require the user to share the PID information in order to issue a pseudonymous attestation of majority. The site/platform requires the user to verify their age by providing them with a QR CODE. By scanning the QR CODE using the digital wallet app, the user receives a request to present the pseudonymous attestation of majority and consents to share the requested information. The website/platform thus receives information on the age of majority from the digital wallet.

#### IV. **Standardisation and regulatory initiatives**

At European or, in general, international level, numerous initiatives have been implemented or are still being developed, an overview of which is provided in **Annex 1** to this document, to which reference is made.

---

<sup>20</sup> The term ‘pseudonym’ means an identifier that uniquely represents a user and that does not contain any reference, data or information about the user’s attributes or personal data.

## 2 ANNEX 1

### I. Standardisation and regulatory initiatives

At European or, in general, international level, numerous initiatives have been implemented or are being developed, an overview of which is provided in Annex 1 to this document to which reference is made.

#### 2.1 I.1 The euConsent project

This is a European project, co-funded by the EU, which involves developing an interoperable, browser-based age assurance method.

As part of the activities of the euCONSENT project, a draft document entitled 'ISO Working Draft Age Assurance Systems Standard' was published.

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

<b>Characterisation of age verification systems</b>
---

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

The age assurance may apply to specific ages or age groups (age-based classification). According to the document, **an age assurance system** is composed of:

- (a) One or more **verification components** which indicate the age of a person,
- (b) A **processing subsystem** that analyses the *confidence level* 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 'strict' in accordance with certain ISO standards), and communicated to a party relying on such verification (in case 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 the age (e.g. over 18 years old). *Attribute* means the characteristic or property of an entity, in this case the age (e.g. over the age of 18).

The **verification components** of 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 using *artificial intelligence* (a branch of computing 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, behaviours, characteristics, or actions of individuals,

(d) A process or system that implements ***social proofing*** (social proofing is the analysis, with the user's consent, of the user's digital footprint and related social graphs, which can be queried to assess the veracity of an alleged self-asserted age assurance) 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 evaluating elements that take into account a person's appearance, behaviour, 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.

One ***processing subsystem*** of the age guarantee may include:

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

(b) A process or system to identify possible attacks by malicious actors, to protect against presentation attacks, to and assess the liveness of individuals,

(c) A process or system for identifying and addressing *contraindicators* (evidence or information that questions or otherwise indicates that the stated age may not be the real one),

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

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

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

(g) A process or system for monitoring, continuous improvement, 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.

One **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 body established for that purpose. Consideration should be given to the inherent risk that the primary credential may have been issued inappropriately, to the wrong person, with incorrect data or may have been falsified.

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

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

### Contraindicators

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 mismatches of data or information indicating that the stated age may not correspond to the actual age. These are called contraindicators.

Providers of age assurance systems have two options when presented with a contraindicator:

- (a) Take action to resolve the contraindicator by gathering additional evidence to support the stated age; OR
- (b) Communicate the existence of the contraindicator to each relying party.

<h3>Classification of age assurance levels</h3>
---

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

#### 1. Assurance Level Zero for age verification

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

Changing the declared age value over time is a so-called contraindicator.

## 2. Basic Level of Assurance for Age Verification

The acquisition of the age declared by the individual is supplemented by the application of at least one age verification component tested at the Evaluation Assurance Level 1 (EAL1, in the draft document there are seven evaluation assurance levels — from EAL1 to EAL7 — which correspond to the increasing efforts for verification and testing of the design).

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

The component of the age assurance process may include simple validation of the declared age attribute. The process must not result in a rate of false acceptances or false refusals of more than 5%.

The basic level provides for systems to reduce attempts at circumvention (attack vector) by bots or automated processes or by false or inaccurate self-declarations, as well as techniques to establish the liveness of an individual. Such attempts should be supported by methods to reduce or eliminate systemic bias in the age verification process. A basic age assurance may leave unresolved contraindicators, which should be communicated to the party relying on verification.

Authentication must be renewed at least every 3 months.

## 3. Standard Level of Assurance for Age Verification

Upon the acquisition of the age declared by the individual, the application of at least one component of the age assurance tested at Evaluation Assurance Level 2 (EAL2) is added.

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

The process of the age assurance component must include validation of the declared age attribute. The process must not result in a rate of false acceptances or false refusals of more than 1%.

If the process is undertaken remotely, liveness of the individual must be established in accordance with ISO/IEC 30107. The non-acquisition rate must be less than 1%.

If the process provides for the use of artificial intelligence, the classification error or statistical parity error due to the specific characteristics of the 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 must recognise false or inaccurate self-declarations. This includes verifying an individual's liveness. Such countermeasures must be based on methods to reduce or eliminate systemic bias in the age verification process.

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

Authentication must be renewed at least every month.

#### **4. Enhanced Level of Assurance for 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) shall be added to the declared age (implicit or actual self-declaration).

The age assurance components must be tested up to Evaluation Assurance Level 3 (EAL3).

The processes related to the age assurance component must include validation of the declared age attribute. The process must not result in a rate of false acceptances or false refusals of more than 0.1%.

If the age verification process is done online, liveness of the individual must be established in accordance with ISO/IEC 30107. The non-acquisition rate must be less than 1%. If the process provides for the use of artificial intelligence, the parity of misclassification or result errors 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 contraindicators must be resolved or communicated to the relying party. Authentication should be renewed at least every week.

#### **5. Strict Assurance Level of Age Verification**

The implicit or actual self-declaration shall be supplemented by the 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.

The age assurance components must be tested up to Evaluation Assurance Level 4 (EAL4). The age assertion may be acquired in a data acquisition process by inviting the user to submit evidence to support the processes of the age assurance components.

The processes related to the age assurance component must include validation of the declared age attribute. The process must not result in a rate of false acceptances or false refusals of more than 0.01%. If the process is undertaken remotely, liveness of the

individual must be established in accordance with ISO/IEC 30107. The non-acquisition rate must be less than 1%.

If the process provides for the use of artificial intelligence, the parity of misclassification or result errors 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 contraindicators must be resolved or communicated to the relying party. The age verification must be repeated for each age-related eligibility decision, repeating the age assurance process.

<b>The security issue: cyber attacks, attempts to circumvent the verification process and contraindicators</b>
--

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) The accuracy, reliability, and risk of fraud of the data source, including consideration of risks associated with the deduction or derivation of 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-wide attack. Therefore, a so-called liveness detection system, as defined by ISO/IEC 30107, becomes important;

Other types of attacks, so-called *Presentation attacks*, can occur:

- (a) through the acquisition of biometric data directly from a person, online or through existing databases, using them for the presentation of biometric spoofing (e.g. a facial image 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 is a forged document (e.g. a forged driving licence, a forged passport or a forged record in a database).

The reliability of the age verification system shall be assessed with respect to this type of attack.



## 2.2 I.2 The public consultation by the UK regulator Ofcom

On 5 December 2023, Ofcom launched a public consultation on guidelines on ‘highly effective’ age assurance to be implemented by online service providers to prevent minors from accessing online pornography services.

Among the age verification methods considered by Ofcom are the following: verification of the correspondence of identity documents with photos, age estimation using facial recognition, and the use of credit cards.

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

The latest research shows that the average age at which children first access online pornography is at 13 years old, although nearly a quarter do so at age 11 (27%) and one in ten at age 9 (10%). In addition, nearly 8 out of every 10 youngsters (79%) had access to violent pornography depicting coercive, degrading or pain-inducing sexual acts before the age of 18.

The Online Safety Act provides that websites and apps that display or publish pornographic content must 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 age assurance methods

Under the above-mentioned law, the Ofcom was mandated to adopt guidelines to support online pornography service providers in fulfilling their legal responsibilities and to oversee implementation. The draft guidelines set out the criteria that age controls must meet in order to be considered highly effective; the criteria are based on the principles of technical accuracy, robustness, reliability and fairness.

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

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

- o **Banking activities.** A user may consent to the sharing of banking information with the online pornography service in order to confirm that they are over 18 years of age. Their full date of birth is not shared.
- o **Correspondence of identification with a photo.** Users can upload an identity document with a photo, such as a driver’s license or passport, which is then compared to an image of the user at the time of uploading to verify that it is the same person.

- o **Facial age estimation.** The characteristics of a user's face are analysed to estimate their age.
- o **Age verification by the mobile network operator.** Some UK mobile operators automatically apply a restriction that prevents children from accessing websites subject to age limits. Users can remove this restriction by proving to their mobile operator that they are of age, and this confirmation will then be shared with the online pornography service.
- o **Credit card checks.** In the UK, credit card issuers are required to verify that applicants are over 18 years of age 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 validity of the card to the issuing bank. Approval by the bank can be considered as proof that the user is over 18 years old.
- o **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.

The Ofcom Guidelines provide examples of approaches to age assurance that do not meet the standards set out in the draft guidelines. Unreliable methods include:

- o the self-declaration of age;
- o online payment methods that do not require a person to be 18 years old (debit cards, Solo or Electron); AND
- o 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 should be understood in a general sense and depends on the methodology used). In some cases, age verification is carried out by estimating the age. In other cases, through 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 to be taken into account by service providers when designing or implementing an age verification system in order 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 not to have complied with age verification requirements.

The following definitions shall apply:

- **age verification method**, the particular system or technology that underlies an age verification process; AND
- **age verification process**, the end-to-end process through which an age verification method or a combination of methods is implemented to determine whether or not 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 controls on access 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 additional 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 results that it is:

- Technically accurate
- Robust
- Reliable
- Fair

**Examples of age assurance methods that Ofcom believes could be very effective are:**

**Open banking**

**Photo-ID matching**

**Age estimation using 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 cannot be effective**

#### **Self-declaration**

#### **Debit cards, Solo or Electron**

#### **Other payment methods that do not require the user to be over 18 years old**

#### **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 in-house by the service provider; others may be provided by third-party providers. These methods work in different ways, and the technology behind them is likely to continue to improve over time. It is also noted that new approaches to age verification are likely to emerge in the future.

For this reason, Ofcom has adopted an approach to the Guidelines that is not aimed at providing 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 that, as far as possible, the Guidelines are future-proof and technology-neutral.

Examples of age verification systems that can be considered effective include some established ones, such as photo-identification matching (photo-ID), 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 according to 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 legal obligations to which reference is made.

### **Description of the criteria to ensure that the age verification system is effective**

Ofcom considers it appropriate, in line with the above, to provide general criteria for assessing whether a given process can be considered effective in relation to the objective of age verification that is as certain 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 indications on the measurement of each of the aforementioned KPIs without defining, at

this stage, the thresholds. However, it asked respondents to provide assessments both in relation to other useful KPIs and in relation to thresholds.

### **Technical accuracy**

The technical accuracy criterion refers specifically to how an age verification method can correctly determine the age of a user in the test environment (e.g. in the laboratory). The term ‘technical’ accuracy has been used to distinguish this criterion from additional 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 in facial recognition or inference of user behaviour. Some studies provide metrics for estimating accuracy. An example is provided in the Age Check Certification Scheme (ACCS) document on age assurance measurement technologies, which examined several parameters for the assessment of age assurance.

### **Robustness**

The robustness criterion describes the degree to which an age verification method can correctly determine a user’s age under unforeseen or actual conditions. In order to meet this criterion, service providers should take the following measures:

- a) ensure that age assurance methods have been tested in multiple environments during their development;
- b) adopt measures to mitigate circumvention methods that are easily accessible to minors and where it is reasonable to assume that they can use them.

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

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

- a) low/different 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 acknowledged that any age verification system may be subject, even successfully, to attempts at circumvention).

It is therefore necessary for service providers to 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 functionality of the age verification method. Reference is made, by way of example, to cases where a minor can obtain

access to pornographic content using the personal data or means of identification of an adult or by otherwise impersonating them<sup>21</sup>.

### **Reliability**

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

For the purposes of a reliable verification system, the service provider shall:

- a) ensure that age verification methods with a certain degree of variance (e.g. methods based on statistical models or artificial intelligence) have been adequately tested and that performance thereof is measured and monitored; AND,
- b) ensure that the evidence used by the age verification method comes from a reliable source.

### **Equity**

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

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

---

<sup>21</sup> Ofcom, in its document, has provided case studies for illustrative purposes.

The first specific example is the one in which the service provider has implemented a method for estimating facial age that requires only a still image. This functionality, without further authentication, risk being subject to 'printin attacks', i.e. when a printed photograph or facial image of a user is presented to the camera to attempt to match the image on the ID document with a photo. 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 assurance process that enables age verification to be done using fake or manipulated IDs (for example, where age could be altered using a pen or pencil on an existing ID at one extreme) or more advanced forms that involve the misuse of authentic documents. The first is easily accessible to children and it is reasonable to expect that they can use it. Therefore, where a regulated service uses a method of matching identity documents with photos, it is necessary for the service provider to take measures to mitigate the most elementary levels of false documentation.

In general, the draft Guidelines acknowledge that there may be other forms of circumvention of the age verification process or the access control process as a whole. Therefore, service providers should 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 process for UK-based users, for example by providing a link to and recommending the use of a VPN to enable them to access pornographic content from regulated providers.

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

#### **Accessibility**

To this end, age verification system should:

- a) be easy to use; AND
- b) function effectively for all.

In order to ensure accessibility, the provider shall:

- a) consider the potential impact that the age verification method(s) chosen could have on persons belonging to protected categories;
- b) consider offering a variety of age verification methods; AND,
- c) design the user's process 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 and standardised formats. It is based on consistent technological approaches adopted in the different systems. Standards, technical frameworks and other specifications are important in order to achieve interoperability.

In the context of age verification, interoperability may involve the re-use of the result of an age check on multiple services, 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.

### ***2.3 I.3 The CNIL's position in France on the balance between the protection of minors and respect for privacy***

In France, the CNIL (an independent administrative authority established in 1978 by the Data Protection Law, the CNIL is composed of a college of 18 members and a group of State contract agents) analysed the main types of age verification systems in order to clarify its position on age control on the internet, and in particular on pornographic websites for which such control is mandatory. It specifies how these publishers could fulfill their legal obligations. However, the CNIL notes that current systems can be circumvented and are invasive, and calls for the implementation of more privacy-friendly models. Below is a summary of what is reported in a recent publication on its own website.



*Inform, raise awareness and prioritise user control over devices*

In general, the CNIL recalls the importance of informing and raising awareness among minors, parents, judicial officials, and staff of the educational community and youth management on good IT practices, given the increasing importance of the use of digital tools in citizens' lives.

Therefore, as part of its work on children's digital rights, in August 2021 the CNIL published general recommendations indicating the requirements established to verify the age of the child and the consent of parents while respecting their private life, in particular, to comply with the obligations of the GDPR and the Child Access to Social Networks Act. Recommendation No 7, in particular, calls for **the structuring of age verification systems around six pillars: minimisation, proportionality, robustness, simplicity, standardisation, and third-party intervention.**

Finally, the CNIL tends to favour the use of devices under the control of users rather than centralised or imposed solutions: in this context, the means of parental control, which leave it up to families to restrict access to sensitive content, seem to respect individuals' rights the most. However, these means are limited: **the law provides that, in some cases, it is the publishers of websites (for example, of pornographic websites) who are responsible for fulfilling the age verification obligations.**

*The multiplication of legal obligations for online age verification*

French law and certain European regulations make the provision of specific services or goods subject to age conditions, which require the sites in question to verify the age of the customer: the purchase of alcohol, online gambling and betting, certain banking services, etc.

For the particular case of websites disseminating pornographic content, the law of 30 July 2020 to protect victims of domestic violence reaffirmed the age verification obligations, codified in Article 227-24 of the Criminal Code. The dissemination of a 'pornographic message' likely to be seen by minors is therefore punishable by criminal law; **The law specifies that age verification cannot be done simply by a declaration by the internet user that he or she is at least eighteen years old.**

The Chair of the Audiovisual and Digital Communications Regulatory Authority (**Arcom**), within the framework of the powers entrusted to him, **in December 2021 ordered several pornographic websites to establish effective age checks on internet users.**

On 3 June 2021, **the CNIL issued an opinion on the draft decree specifying, for the application of the law of 30 July 2020, the obligations of websites that disseminate 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 sites:

- **no direct collection of identity documents by the publisher of the pornographic site;**
- **no age estimation 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 (for example, by comparing, using facial recognition technology, a photograph on an identity document with a self-portrait or a selfie).**

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

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

### **CNIL Recommendations and Warnings on Online Age Verification**

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

##### Age control criteria that raise important issues

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

- On the one hand, **the issuance of a proof of age**: the establishment of a system to validate information on the age of the person by issuing proof of age accompanied by a confidence level. This proof can be issued by different entities who know the Internet user, whether they are **service providers specialized in the provision of digital identity, or an organisation that knows the Internet user in another context** (a merchant, a bank, an administration, etc.). Several solutions are analysed in this document.
- On the other hand, **the transmission of such certified proof of age to the site visited** so that the latter may grant or deny access to the requested content (it should be noted that, as indicated in the PEReN note, a third step is to analyse the proof of age submitted and decide whether to provide access to the requested content).

These two aspects involve important data protection and privacy issues to preserve, in particular, the possibility of using the Internet without revealing one's identity or data which directly identifies oneself. **Entrusting these functions to different entities enables a three-fold protection of privacy:**

- The entity that **provides the proof of age knows the identity of the Internet user but does not know which site is being consulted**;
- The entity that sends the proof of age to the site may know the site or service that the Internet user is consulting but does not know their identity (in the ‘ideal’ solution developed by the CNIL, the proof of age passes through the user, which allows compartmentalisation between players);
- the site or service knows the age of the Internet user (or only that they have reached the age of majority) and knows that they are consulting this site, but does not know their identity and, in some cases, the age verification service used.

#### An independent third-party verifier to better protect individuals’ data

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

The work of the European Commission is moving in this direction, as shown in the Communication entitled “New European Strategy for a better internet for kids” (PDF), in particular in the context of the proposal for a European Digital Identity.

#### Necessary assessment of proof of age by third-party providers

In addition, it also seems necessary, in general, that proof of age providers are subject to a third-party evaluation, especially when adopting an approach based on automatic or statistical analysis.

To this end, and in view of the sensitivity of the data collected and the invasive nature of age verification systems and, more generally, of the processing of identity-related information, the creation of a specific label or certification for these third parties could help ensure the GDPR compliance of means (compliance with the principles of data minimisation, security of the data collected, and purpose limitation).

#### **A necessarily imperfect verification**

As regards the verification processes offered on the market, the CNIL points out that currently all the proposed solutions can be easily circumvented. In fact, using a simple VPN that locates the Internet user in a country that does not require such 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 proof of age is the one who obtained it.

Thus, in the United Kingdom, where such measures have long been considered, 23% of minors state they can bypass blocking measures, and some pornographic content publishers already offer VPN services. If the use of VPNs must be subject to some

vigilance, it should be emphasized that these technologies are also one of the essential elements of the security of exchanges on the Internet, used by many companies but also by private individuals who want to protect their browsing from tracking carried out by public or private entities.

#### Analysis of existing solutions

The CNIL has analyzed several existing solutions that allow for the verification of the age of online users, checking whether they have the following properties: **a sufficiently reliable verification, comprehensive coverage of the population, and respect for data protection and the 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 players in the sector to develop new solutions, following the recommendations developed above. The CNIL considers it urgent that more effective, reliable and privacy-friendly systems get proposed and are monitored as soon as possible. Article 3 of Decree No 2021-1306 of 7 October 2021 entrusts ARCOM with the task of developing guidelines that describe in detail the reliability of the technical processes that websites must implement to prevent access by minors.

However, measures are already in place to improve the level of protection of minors, in particular the youngest among them. Several solutions are described below, in descending order of maturity from the point of view of the CNIL. Pending the establishment of adequate checks and only for a transitional period, the CNIL considers that some of these solutions could make it possible to enhance the protection of minors, provided that they are guaranteed of their implementation and in particular of the additional risks generated by their use.

#### **1. Age verification via payment card validation**

Payment card age verification has the advantage of relying solely on infrastructures that have already been implemented and tested. It is therefore considered, even though this type of verification may be circumvented (since minors may be in possession of payment cards that allow them to make purchases on the Internet) and are not accessible to everyone (since adults may not possess 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 and not on a payment, although some propose a micropayment, that is immediately cancelled.

Such a system makes it possible, in particular, to protect young people (approximately until they begin secondary school), who cannot have a bank card that allows them to make an online payment.

On the one hand, this age verification system should not, in principle, be implemented directly by the controller (i.e. the website consulted) 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 phishing risks 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 site publishers and solution providers to launch a campaign in parallel to raise awareness of the risks of phishing, taking particular account of this new practice. Free access must remain so: the use of this system must not involve any cost to the user.

## **2. Age verification by estimation based on facial analysis**

Some age estimation processes are based on facial analysis, but do not aim to identify the person. However, it is necessary for those who dispute the outcome of the verification to have another method of verification.

The use of such systems, due to their invasive nature (access to the user's device's camera during the initial registration with third parties, or a random check by those same third parties that 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 evaluation, should be mandatorily subject to compliance with reliability and performance requirements independently verified by a third-party entity.

According to the CNIL, preference should be given to an age estimation carried out locally on the user terminal in order to minimise the risk of data leakage. In the absence of such a requirement, this method should not be used.

## **3. Offline verification system**

The offline verification method which seems to be the most successful appears to be the marketing to adults only of 'scratch cards' that allow them to retrieve an identifier and password that would provide access to age-restricted content. These cards would be offered at certain points of sale, such as supermarkets or tobacconists, where their employees already carry out age verification operations in the context of the sale of alcohol, cigarettes, and gambling.

However, this method cannot be used exclusively for the consultation of pornographic sites, as it could be stigmatising for the person concerned. All age-restricted activities should be included and this model should be promoted by a diverse community of publishers (purchases of regulated products, pornography, etc.). The limits of such a system would be the same as for the purchase of cigarettes or alcohol, i.e. fraud by reselling cards on a parallel market.

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

#### **4. Age verification through the analysis of identity documents**

Age verification may be carried out by a third party responsible for collecting and analysing 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 needed (the possibility of using another adult's document, even within the same household). This system is therefore unreliable and disrespectful of personal data, because it requires, in order to function, the collection and processing of official identity documents.

Some systems verify the identity of the person by comparing the photograph of the identity document provided with a 'live detector' test, i.e. the capture of a photograph or video taken by the person of the user at the time of verification of the age requirement, in order to verify that the user is indeed the person they claim to be and to counter possible circumvention of the means. This process is much more reliable and is also used for identity verification according to the ANSSI PVID standard.

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

Prerequisites: as with the PVID standard, it is necessary to set up a certification body (or labelling) to verify that the necessary guarantees are in place for the collection and analysis of identity documents.

#### **5. Use of tools offered by the State to verify identity and age**

The use of public databases or of an authentication system such as FranceConnect could theoretically allow one to prove their age to access certain online sites or services. However, FranceConnect was not designed for this purpose, but with the aim of simplifying administrative procedures: its very functionality is based on the recording of uses on State servers. This method does not therefore appear to be satisfactory, as it would lead the State to have a list of connections of a purely private nature. Furthermore, as regards the consultation of pornographic websites, the use of these means would entail 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 identity systems of the State could be considered.

Prerequisites: it is necessary to use trusted third parties that connect attribute management services to the identity systems of the State.

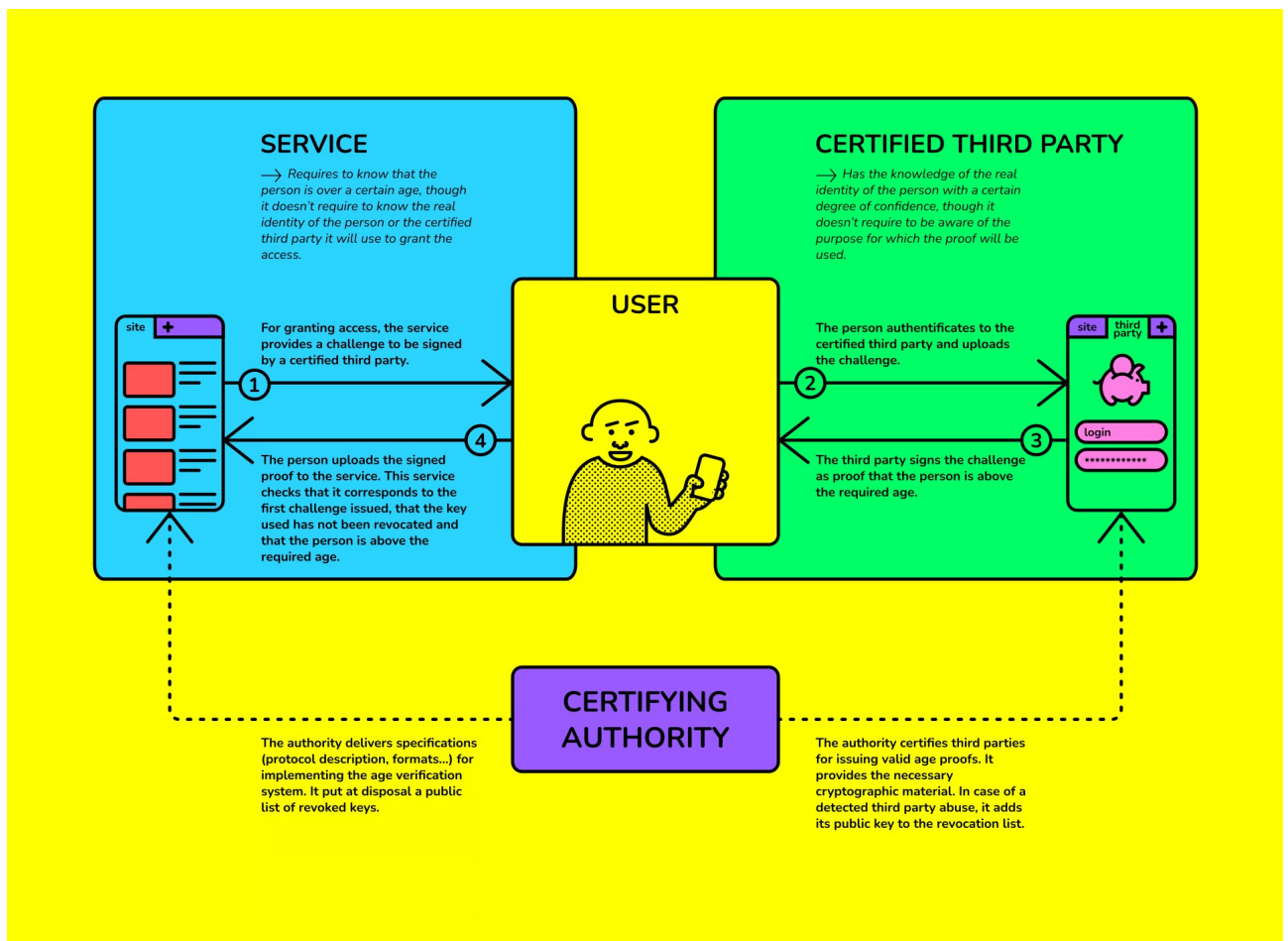
## 6. Inferential age verification systems

There are three main variants of this type of analysis: the first hardly appears to be compatible 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 navigation data.

- Importing the individual's Internet browsing history: this method seems too intrusive for the simple purpose of age verification.
- 'Maturity' analysis by means of a questionnaire: this method seems to avoid the transfer of personal data. However, this method seems to be reliable only relatively, and the possibility of circumvention (sharing responses online) is significant, as well as the biases that could be associated with it. For example, a part of the population could be discriminated against on the basis of their skills (reading, comprehension), their level of knowledge of the language, their cultural references, etc. This method should therefore be avoided.
- Analysis of navigation on the specific services of the site publisher (particularly for large digital platforms). Re-use of data for the creation of age inference (or deduction) models seems possible, subject to the following points:
  - o in principle, this method should not lead to an automated decision, but to a preliminary estimate which, in case of suspected non-compliance with the age requirement, may lead to an exchange with the Internet user;
  - o no additional data shall be collected for the sole purpose of constructing the model (only data already collected shall be used);
  - o The data produced on the platform's services must be distinguished from the data collected by tracking the user's navigation on other sites (for example, through authentication on the platform, by installing a mechanism to track access to certain web pages, etc.);
  - o The inference system should be assessed 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 an encryption-implemented process that allows identified individuals to prove that a situation is true without having to disclose other information. It has been demonstrated that it is possible, through a third-party system, to ensure the protection of the individual's identity and the principle of data minimisation, while maintaining a high level of assurance on the accuracy of the data transmitted. However, it is assumed that the third parties used are completely independent of the publishers.





#### 2.4 1.4 The 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 22 July 1992, it is forbidden to expose minors to pornographic content. Article 23 of Law No 2020-936 of 30 July 2020, aimed at protecting victims of domestic violence, entrusted the Audiovisual and Digital Communications Regulatory Authority (Arcom) with the prerogative of warning public communication services that do not comply with this criminal obligation, as well as referring to the courts in order to block sites that do not comply with the aforementioned warning.

The French law known as the PJJ SREN, aimed at securing and regulating the digital space, provides for granting Arcom the power to administratively block online public communication services with editorial responsibility and the services of video-sharing platforms that disseminate pornographic content accessible to minors after being sentenced to comply with Article 227-24 of the Criminal Code. That power, exercised in the context of a special procedure under the control of the administrative court, complements the powers otherwise conferred on the judicial court in this matter.

In addition, the law provides that **Arcom shall adopt a framework, after consulting the National Commission for Informatics and Liberties (CNIL), to determine the minimum technical requirements applicable to age verification systems set up for access to services that disseminate pornographic content.** Failure to comply with the requirements entails a financial penalty, following a warning by Arcom.

On 11 April 2024, Arcom published the **Public consultation on the draft framework laying down the minimum technical requirements applicable to age verification systems implemented for access to online pornographic content**, in anticipation of the adoption of the P.J.L. SREN law.

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

### **Robustness of the solution**

The protection of minors must be the default, starting with the display of the first page of an online public communication service that allows the dissemination of pornographic content. Online services that broadcast pornographic content are required to display a screen that does not contain pornographic content ‘provided that the age of the user has not been verified’.

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

Publishers may indicate the pornographic nature of their service. In order to do so, they can rely on a self-declaration mechanism (e.g. labelling each web page as ‘for adults only’), enabling 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 to be made between underage and adult users.

### **Limitation of the possibility of circumvention**

Services that disseminate pornographic content must do their best, in accordance with the industry’s high standards of professional diligence, to limit the chances of circumvention of the technical solutions they implement. Age verification systems should not allow the sharing of proof of age with other persons. Finally, the system must be robust against the risks of attacks, such as deepfakes, spoofing, etc.

For example, for solutions based on age estimation through the analysis of facial features, services transmitting pornographic content must ensure that the solutions contain a mechanism for the recognition of living organisms, the effectiveness of which is in line with the state of the art. Detection must be carried out with sufficient image quality and must allow for the exclusion of 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 that it is not a mere copy; (ii) that the user is the holder of the identity document provided. Such verification may be carried out, in particular, by recognising facial features by means of a liveness detection mechanism, under the conditions set out above.

### **Age verification every time the service is consulted**

The age verification must be done each time a service that disseminates pornographic content is consulted. After the consultation of the service is interrupted, a new age verification must be triggered in the event that the pornographic content is accessed again.

Compliance with this criterion shall be without prejudice to the possibility for the user to use reusable or self-regenerated proofs of age, subject to the presence of a second authentication factor. This can be done by linking the use of the reusable proof to the terminal of the person concerned, as in the case of digital wallets. In addition, the verification system must not allow this evidence to be shared with another person or with another service.

For example, in the case of a device shared between an adult and a minor, it is appropriate to avoid that the validity period of the age verification allows the viewing of pornographic content without further verification. The validity of an age verification must therefore cease when the user leaves the service, when the session ends, when the user exits the browser, or when the operating system enters 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 should not require the creation of a user account on the service in question that makes pornographic content available. In addition, proof of age cannot be stored in a user account on that service. In any case, the age verification obligation applies to each access, with or without a user account.

### **Non-discrimination**

The solutions adopted by the 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 systems for generating proofs of age based on machine learning or statistical models, service providers can, for example, test their solution on different databases to ensure compliance with this requirement.

It is essential that age control systems limit discriminatory bias, which also generates errors that call into question both their reliability and acceptability.

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

### **Protection of personal data**

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

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

- o accuracy, proportionality and minimisation of the data collected;
- o concise, transparent, comprehensible and easily accessible user information;
- o appropriate data storage periods;
- o the possibility for data subjects to exercise their rights, i.e. the right of access, the right to object, the right to rectification, the right to restriction of processing, the right to erasure, the right to data portability;
- o state-of-the-art security of information systems used in the processing of personal data.

In 2022, the CNIL published an example of a privacy-friendly age verification mechanism for transmitting an identity attribute (in this case the 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 its technical feasibility and ability to respond to the need for privacy protection inherent in online age verification mechanisms to be confirmed. It also corresponds to the objectives generally set for digital identity systems, including attribute management. However, this mechanism, although referred to as ‘double anonymity’, is not entirely ‘anonymous’ within the meaning of the GDPR, but nevertheless ensures a high degree of confidentiality.

Online public communication services that make pornographic content available must offer their users at least one age verification system that complies with privacy protection rules on ‘double anonymity’, ensuring that this system can be used by the vast majority of their users.

This requirement shall enter into force at the end of the transitional period provided for by 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 provided 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 basis of requirements applicable to all age verification systems covered by the proposed regulation.

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

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

#### **Confidentiality with respect to services disseminating pornographic content**

Personal data, which allow the user to verify their age with a communication service covered by this proposal for a regulation, must not be processed.

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

#### **Confidentiality regarding providers generating proof of age**

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

#### **Confidentiality with regard to any other third parties involved in the age verification process**

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

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

When determining whether a user can access an online public communication service based on the proof presented to it, the concerned service disseminating pornographic content shall make an automated decision pursuant to Article 22 of the GDPR. By refusing access to a service, that decision is liable to produce legal effects on the persons concerned, or at least to produce significant effects which affect certain persons in a similar way.

The CNIL considers that this decision can be based on the exception provided for in paragraph 2(b) of Article 22 of the GDPR, to the extent that the service in question that disseminates pornographic content is subject to the age verification obligation provided for in Article 227-24 of the Criminal Code and, ultimately, by the provisions of the PJJ SREN. Article 22(2b) of the GDPR requires that appropriate measures to safeguard the

data subject's rights, freedoms and legitimate interests be provided for in the provisions authorising such automated decision-making.

In order to preserve privacy requirements that aim to limit the ability of services to identify individuals, such measures must be put in place not by the service in question disseminating 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 enable users, in the event of an error, to dispute the result of the analysis of their characteristics in order to obtain proof of age. To exercise those remedies, providers of age verification solutions should offer users the possibility to use different providers of attributes or, depending on the solution, different issuers of evidence.

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

In any case, providers of attributes must also allow individuals to rectify their data pursuant to Article 16 of the GDPR.

#### **Enhanced confidentiality regarding the targeted services disseminating pornographic content**

An age verification system using 'double anonymity' must not allow the communication services covered by the Regulation to recognise 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 using 'double anonymity' must not allow these services to know or infer the source or method for obtaining the proof of age involved in the process of verifying a user's age.

An age verification system that respects 'double anonymity' must not allow these services to recognize that two proofs of age come from the same source of proof of age.

#### **Enhanced confidentiality with regard to entities providing proof of age**

An age verification system using 'double anonymity' must not allow proof of age providers to know for which service age verification is being performed.

#### **Greater confidentiality with regard to any other third parties involved in the age verification process**

An age verification system using 'double anonymity' should not allow any other third party involved in the process to recognise a user who has already used the system. For example, a third party that ensures the transmission of proof of age or certifies its validity should not be able to know if it has already processed the proof for the same user.

#### **Availability and coverage of the user population**

Regulated communication services must ensure that their users have at least two different methods available to generate their proof of age, enabling the proof of age to



be obtained through a ‘double anonymity’ age verification system. In practice, a service provider offering a double anonymity solution must combine at least two methods to obtain proof of age (e.g. a solution based on identity documents and a solution based on age estimation).

The communication services covered by this rule must ensure that a ‘double anonymity’ age verification system is available for at least 80% of the adult population residing in France.

#### **Explicit information on the level of protection of users’ privacy**

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

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

For age verification systems that respect 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 such verification is being carried out.

#### ***Non-mandatory requirements and good practices***

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

##### Possibility for the user to independently generate a proof of age confidentially:

- o The user can generate a proof of age locally, without informing the initial issuer of their age attributes, nor another third party;
- o The user can generate a proof of age through an online service that can be used without having any access to their personal data.

##### Confidentiality of age verification systems as a whole:

- o the system is based on zero-knowledge proofs;
- o the system is based on encryption techniques that are resistant to the most complex attacks, even future ones

#### ***Derogatory proof of age solutions accepted on a temporary basis***

The French regulator provides 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 laid down, bank card solutions will be deemed to comply with the technical characteristics of the framework, subject to compliance with the following conditions.



A solution using bank cards will constitute an initial method of filtering a portion of the minors.

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

These verification systems:

- o must not be implemented directly by the targeted services that distribute pornographic content, but by a third party independent of the service;
- o must ensure the security of the verification, in order to prevent the phishing risks associated with it. It is therefore important to ensure that payment information is entered correctly on trusted sites. In this regard, the targeted services disseminating pornographic content and the solution providers should launch a coordinated campaign to raise awareness of the risks of phishing, taking particular account of this new practice;
- o they must at least make it possible to ensure the existence and validity of the card, excluding a simple verification of the congruence of the card number;
- o shall implement strong authentication as required by Directive (EU) 2015/2366 on payment services (so-called ‘DPS2’), for example by relying on the 3-D Secure protocol, in its second version in force, to ensure that the user of the service is the cardholder by means of two-factor authentication.

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

## **2.5 I.4 The public consultation by the Spanish regulator**

The Spanish Regulatory Authority (CNMC) has launched a *Public consultation on criteria to ensure the adequacy of age verification systems on video-sharing platform services for content harmful to minors*.

In the national regulatory context, Spanish Law 13/2022 of 7 July on general audiovisual communication (*Ley General de Comunicación Audiovisual*; hereinafter ‘LGCA’) has extended the subjective scope of regulated entities, audiovisual media service providers, and 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, in particular terrorism.

Article 89 of the LGCA imposes a number 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 purpose of this consultation is 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 video-sharing platforms (VSPs) aimed at disseminating content that is inherently harmful to minors, such as violence or pornography, is a matter of social concern. This is especially so when this type of content is made accessible to minors, as it can alter their ability to understand and compromise their physical, mental, or moral development. In this context, it points out that the development of the new European audiovisual regulatory framework 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 were transposed into Spanish law through the LGCA of 7 July 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.

### **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 operate systems to verify the age of users with respect to content that may impair 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 behaviour 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 applies 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 the analysis of the different age verification services, as well as experience in France and Germany, the regulator proposes a number of minimum elements that the different 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 the harmful content is an adult.

Given that access to this type of service tends to be recurrent, it will be necessary to ensure that the person who initially verifies the age of majority will also be the only one able to use this verification to access the service in the future.

In other words, the verification system must ensure that the person seeking to access the content is indeed the individual identified as an adult, preventing possible cases of identity theft or system breaches.

Identification and authentication may be carried out on the basis of **identity documents or digital certificates**. In some cases, prior registration is possible, where the age of the member is identified, followed by a subsequent check to ensure that the person (previously identified) is the one being authenticated to access the service.

The age verification mechanisms will be divided into two phases: the first phase corresponds to the unique identification of the person, the second phase to an authentication confirming that it is the person previously identified who is accessing the adult service in each subsequent use.

- The first step of the unique identification concerns 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 card, passport), comparing the photograph or fingerprint.

However, the technological progress observed in the formulation of this type of solutions seems to make **the need for 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 between the possibilities that are offered to them.

The regulator considers it reasonable **to reject some solutions as inadequate, such as simply presenting or sending a copy of the identity document, as well as identifying and verifying one's age by presenting a photograph**, as they do not provide adequate safeguards.

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

- The second stage of authentication is to ensure that only the identified person in this way and whose age has been verified has access to the service in question.

To this end, authentication must take place at the beginning of each use or login process and access to content must depend on an individually assigned authentication element. Moreover, since in most solutions, after the unique identification, the user, recognised as an adult and therefore authorised, receives a form of 'password' for all subsequent use processes, the possibility of transferring access authorisations to unauthorised third parties should be

prevented. The disclosure or multiplication of passwords can be prevented by technical measures that make it difficult to multiply access permissions, but also by informing the user of the personal risks arising from the unauthorised use of their password.

**The system must be robust and accurate in order to avoid possible identity theft.**

Regardless of the type of identification carried out, it is essential that the elements of judgment applied make it possible to ensure that the identified person is of majority age.

**Technological neutrality**

Given the different ways of accessing pornographic, violent, and other harmful content, the age verification system should be able to be used on any technological device and operating system, in such a way that minors cannot circumvent controls and access content.

## **II. Technological solutions available for age verification**

The regulator considers that the mere declaration of being of majority 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 the reliability with which it prevents minors from accessing content, subject to compliance with the legislation on the protection of personal data. Technical solutions can be broadly grouped into two types. The following will illustrate the main characteristics of each one, specifying, where appropriate, the possible disadvantages of each.

### **A. Verification of age by means of an identity card or digital certificate deriving therefrom**

- Age verification can be done 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 the true and actual identity, it is possible to provide for **the use of credentials for reaching the age of majority**, such as those provided for in the forthcoming eIDAS Regulation, based on a **digital identity**. In this way, this legal age can be independently verified without the need to disclose further information about the user, in compliance with the principle of data minimisation, and while preserving the user's anonymity.

As far as authentication is concerned, *face to face* or remote procedures could be used that are based on keys, fingerprints or photographs of the person.

Some authentication solutions involve bringing the face closer to the camera of the device with which you are requesting age verification, to ensure that a photograph is not used.

In face-to-face solutions, adults **can obtain cards that are for adults only, through which they receive a username and password** that would allow them to access age-restricted content. Such cards would be offered at certain points of sale, such as supermarkets or tobacconists, whose staff are aware of the age checks relating to the sale of alcohol or cigarettes. The main disadvantage is that such a measure introduced solely for viewing pornographic or violent sites could stigmatise the individual concerned and discourage their use. 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 another.

#### **B. Age verification via bank card**

In existing solutions of this type, users enter their name and bank card details (card number, expiration date, CVC code) and this data is compared with a payment database to verify that the card is valid. It could be a simple check that the number provided is in the correct format, a request for pre-authorisation 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 of age) who do not have a bank card that allows them to make an online payment 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 be in possession of 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 tied to a certain income.

### **III. On organisations that could carry out age verification**

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

In this sense, independent age verification organisations can also be used for purchasing alcohol or tobacco or for enabling online gambling. In addition to the examples given above for proving legal age, third-party verifiers are widely used by telecom companies

and banking organisations to validate their customers' data before entering into online contracts.

In this way, the third party providing the 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 owner knows that the user is of age, but does not know any other personal information or information related to the identity of the user. It is necessary to clarify that the user must know whether the third party is independent of the service provider to whom they request access and to monitor the possible economic links between the third parties and the service providers.

#### **IV. On further aspects to be satisfied by the age verification**

Additional security aspects of the age verification mechanisms should be considered, such as the existence of backdoors, the maximum duration of a session, or the time limit for considering one as inactive. Another aspect to consider among all the possibilities available on the market for age verification is to choose a service that adequately collects age data in the least invasive way possible, respecting individuals' privacy.

#### **V. Summary of contributions to the public consultation**

The National Commission on Markets and Competition (CNMC), in April 2024, published a summary of the contributions<sup>22</sup> 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 Law on Audiovisual Communication, is competent to assess whether the systems used by video platforms established in Spain do prevent minors under 18 years of age from accessing harmful content — pornography and gratuitous violence — when verifying the age of their users.

In the public consultation process, 35 contributions were received from virtually all players related to this sector: user associations, media, audiovisual agents, providers of age verification systems, verifiers or video exchange platforms (PIVs).

##### **Scope of the prohibition on access**

All responses agree that age verification systems (AVS) must cover both content and related advertising, as they also violate children's rights. 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 hosted on a general or a pornographic platform, and that AVS should be applied before access to content (65%) is allowed, regardless of the type of platform.

---

<sup>22</sup> <https://www.cnmc.es/prensa/respuestas-cp-verificacion-edad-plataformas-20240417>

### **Freedom in the choice of age verification systems**

Most contributions (83%) say that there should be several AVS and that the platform should choose which one to implement. This approach not only benefits platforms, which can choose the AVS that suits their business model, but also responds to different user needs (different 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 sector are:

1. Verification via an identity document and comparison with a photo (selfie)
2. Age estimation by facial analysis.

### **Balancing system suitability and data protection**

The majority considers that data protection is a determining factor for the effectiveness of the AVS. Anonymity in accessing content has been highlighted by several agents and, in line with this, the European Digital Wallet (eIDAS2) has been indicated as ideal for this process, as it allows verification of only the age of majority without sharing more data.

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

### **Third parties that may carry out age verification**

92% prefer it to be an independent third party. This option is based on the fact that there are already verification agents on the market that perform this function safely, while respecting data protection and transparency for the user. In addition, having the verification performed by a third party generates trust among users.

### **Self- and co-regulation tools**

81% understand that it can be a very useful tool since it involves the industry, allows greater flexibility and rapidity of adaptation to changes, and can also contribute to the creation of standards. On the contrary, this system is perceived as slow to build.

## **2.6 1.5 German regulation**

The German regulatory authority Kommission für Jugendmedienschutz (KJM) established criteria in May 2022<sup>23</sup> for the assessment of age verification systems.

---

<sup>23</sup> The KJM website for age verification systems <https://www.kjm-online.de/aufsicht/technischer-jugendmedienschutz/anzulaessige-angebote/altersverifikationssysteme>



These are based on the concept that some pornographic content, which is harmful to minors, can only be distributed on the Internet if the provider ensures that only adults can access it through so-called age verification systems (AV systems).

The requirements for such AV systems are significantly higher than the technical requirements for generic access to content, as they must ensure that an age check via personal identification is carried out.

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

Details regarding the evaluation grid are published in the document ‘criteria for the evaluation of concepts for age verification systems’<sup>24</sup>.

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 generally must be done through personal contact. The prerequisite for reliable age verification is the personal identification of natural persons, including verification of their age. Personal identification is necessary to avoid the risk of counterfeiting and circumvention.
- b) through **authentication during individual use 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/transfer access permissions to unauthorised third parties.

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

The KJM evaluation grid enables transparent processes for providers and includes the following cases:

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

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

In addition, procedures may be sufficient to determine the age of majority with a high degree of probability (plausibility check). Contrary to the concepts of

---

<sup>24</sup> The KJM criteria for age verification systems are published online on the following link (in German) [https://www.kjm-online.de/fileadmin/user\\_upload/KJM/Aufsicht/Technischer\\_Jugendmedienschutz/AVS-Raster\\_ueberarbeitet\\_gueltig\\_seit\\_12.05.2022\\_004\\_.pdf](https://www.kjm-online.de/fileadmin/user_upload/KJM/Aufsicht/Technischer_Jugendmedienschutz/AVS-Raster_ueberarbeitet_gueltig_seit_12.05.2022_004_.pdf)

reliable age verification for repeated use (see below), the entire procedure must be performed with each use.

This can be achieved, for example, through a procedure in which the user is examined **through a webcam**, provided that only suitably trained personnel are used, and that effective liveness detection and sufficient image quality are ensured. Liveness detection and sufficient image quality are necessary to ensure that a real person is sitting in front of the camera and to rule out possible circumventions, such as the use of recorded footage or masking. If the user is clearly not of age, an additional identity check must be carried out. If the identity check is carried out via webcam, the above requirements also apply.

It is also necessary to ensure that **the identity card** is checked from all sides and entirely. If it is not possible to establish with certainty that the user is of age, access may not be granted.

However, the mere verification of the ID card code or the presentation of a copy of one's identity document is not sufficient. Even a certified copy of the identity document is not sufficient, as it only confirms that a document corresponds, but does not identify a person.

## **2. Age verification concepts 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 the unique identification, the user who has reached the age of majority and is therefore authorised is assigned a sort of 'general key' for all subsequent use processes. This gives him 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 satisfy the requirements in this case.

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

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

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

It is also possible, under certain conditions, to resort to a 'face-to-face' check that has already taken place. This is the case, for example, for identification procedures using verified personal data, age or birth data, which are used when accessing certain services or entering into certain contracts (e.g. mobile phone contracts, opening bank accounts, etc.).

Face-to-face checks between those present can be dispensed with if identification is done through software by comparing the biometric data reported on the identity document and a photo of the person to be identified, as well as automatically recording the data on the identification document.

The face-to-face check of those present with comparison of official identification data (identity card, passport) may be waived if a procedure based on automated age determination via camera is used for age verification. The software formulates statements on the probability of the age of the person to be identified based on the biometric characteristics of a live camera image and thus reaches 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 necessary for age verification should be recorded and stored to the extent necessary in accordance with data protection rules (e.g. date of birth, name, address).
- C. Requirements for collection points: Identification data can be collected at different points (e.g. post offices, various points of sale such as mobile operator shops, lottery points, 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, concrete location).
- D. Final age check: Access to the closed group of users (activation of user data for authentication) can only occur if the AVS provider receives the identification data or a reference to them and verifies their age.

Finally, with regard to **Authentication**, aimed at ensuring that only the identified and age-verified person can access closed user groups and at making it more difficult to transfer access authorisations to unauthorised third parties, the requirements provide for:

- A. Authentication at the start of each use process ('session');
- B. Content protection by means of a special individually assigned password.

## 2.7 1.6 The public consultation by the Irish regulator

The 'Coimisiún na Meán' (hereinafter the Commission) is Ireland's regulatory body for broadcasting, video on demand, online security and media development and deals, *inter alia*, with setting standards, rules and codes for the different types of media services and related online services under the jurisdiction of Ireland.

On 8 December 2023, the Commission launched a public consultation.<sup>25</sup> which provides for the proposal of an ‘Online Security Code’ for video-sharing services and platform providers (hereinafter ‘VSPS’ or ‘VSPS providers’).

### **Online Security Code proposed by the Irish Commission**

One of the main tasks of the Commission is to develop an online security 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 Security Code with the aim of ensuring that VSPS providers take appropriate measures to protect minors from harmful content, including illegal content and age-inappropriate content. It also aims to protect the general public from content such as incitement to violence or hatred, provocation to commit a terrorist offence, dissemination of child sexual abuse material, racism or xenophobia crimes, as well as certain commercial communications.

Under the Code, the Commission has specified some important definitions to frame the context, so that the obligations towards VSPS providers allow effective measures to be taken to provide adequate protection against possible harm to minors, as defined by the AVMSD:

#### **Age verification techniques**

VSPS providers are required to adopt effective age verification or age estimation measures and to establish a mechanism to assess their effectiveness.

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

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

With reference to **age verification techniques**, the Commission’s Online Security Code requires video-sharing platform service providers to implement effective measures to ensure that content classified as unsuitable for children cannot normally be seen by children.

---

<sup>25</sup>

Available

online

[https://www.cnam.ie/wp-content/uploads/2023/12/Draft\\_Online\\_Safety\\_Code\\_Consultation\\_Document\\_Final.pdf](https://www.cnam.ie/wp-content/uploads/2023/12/Draft_Online_Safety_Code_Consultation_Document_Final.pdf)

These measures shall be applied at the moment of subscription to the service or upon each access to such content and can be implemented by using age estimation or age verification, as appropriate, or by other technical measures.

Age self-declaration by users of the service is not in itself an effective measure.

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

- content consisting of pornography, or
- content consisting of realistic representations or effects of serious or gratuitous violence or acts of cruelty,

must implement in-depth age verification techniques both for registering an account with the service or for 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 provides that providers of video-sharing platform services ensure that the personal data of minors collected or otherwise generated by them in the implementation of age verification obligations are not processed for commercial purposes, such as direct marketing, profiling and targeted behavioural 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 via tokens by third parties;
- systems based on artificial intelligence and biometrics;
- rigid identifiers such as passports.

The Code requires the use of age verification techniques that are effective in ensuring that minors are not normally able to access services or parts thereof 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 minimise 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 lower if the error is made in the case of a minor close to adulthood.

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

## **2.8 I.7 The Spanish Data Protection Agency (AEPD) – age verification**

The Agency has defined a decalogue (<https://www.aepd.es/guias/decalogue-principles-age-verification-minors-protection.pdf>) of principles that age verification systems must respect in order to protect minors from inappropriate content. The aim is to ensure the protection of minors, respecting the principles, rights and obligations under the GDPR. The decalogue includes the following principles:

- No user identification and tracking of minors
- No information on the ‘status’ of a minor
- Ensuring anonymity
- Checks applicable only to inappropriate content
- Ensuring the accuracy of verifications
- No user profiling while browsing
- No traces or connections of the activities carried out by online users
- Ensuring the respect of fundamental rights online
- Defining the governance framework

In order to demonstrate that there are solutions capable of complying 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 is demonstrated that the identity providers currently implementing the right to personal identity of 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.

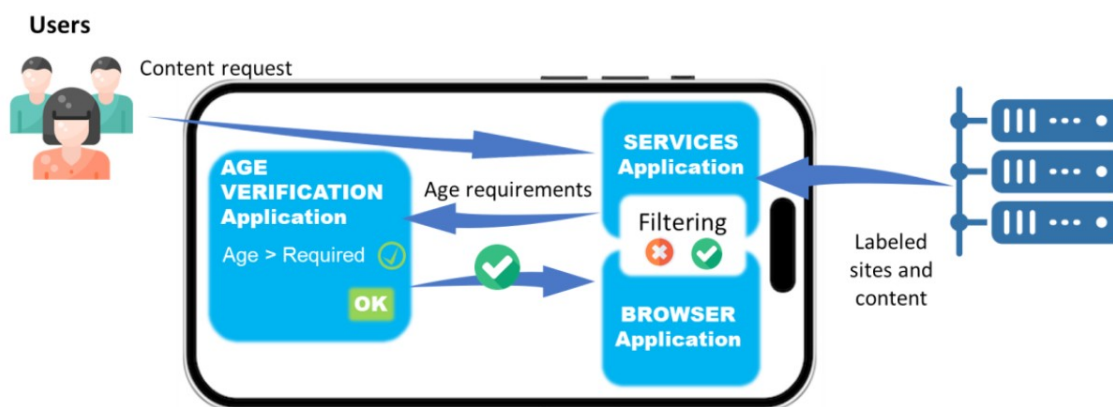
Proof of concept is also based on the fact that protection from inappropriate content can be carried out on the user’s device, with people having complete control over their identity and age, so that systems are fully verifiable and transparent.

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

### Description of the system

1. All content is classified as being ‘all audience’, ‘for adults’, ‘inappropriate for minors’. In the latter two cases, the content is displayed by the internet browser or a content app only after age verification.
2. An age verification App installed on the user’s device is implemented. The age verification App receives the requests referred to in point (1), e.g. via a QR Code displayed by the internet browser or directly via the digital wallet installed on the mobile phone. The App verifies the age of the user and gives the browser permission to access

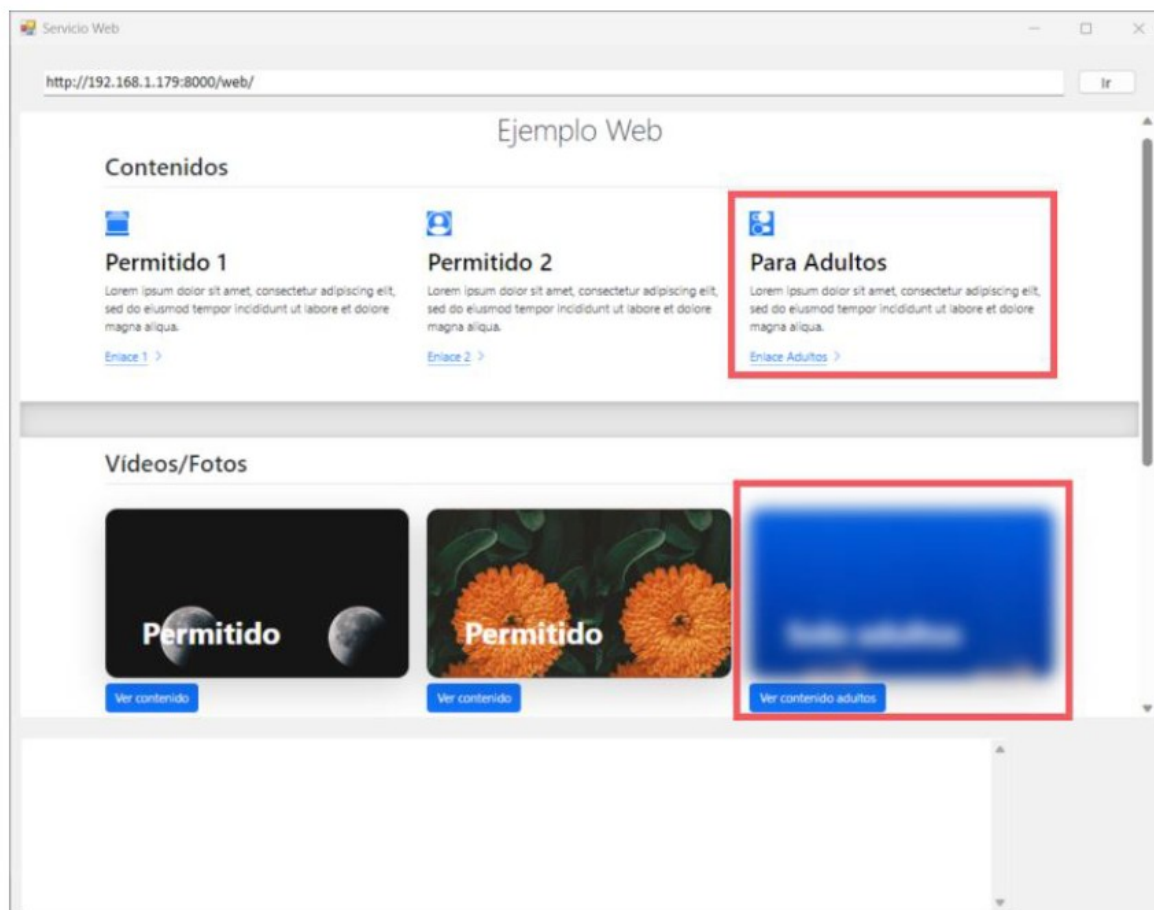
Here is a brief outline:



*High-level description of the system implemented in the PoCs*

The browser hides web content labelled as ‘for adults’, ‘inappropriate for minors’ as shown in the following image. Age verification is required to access it.



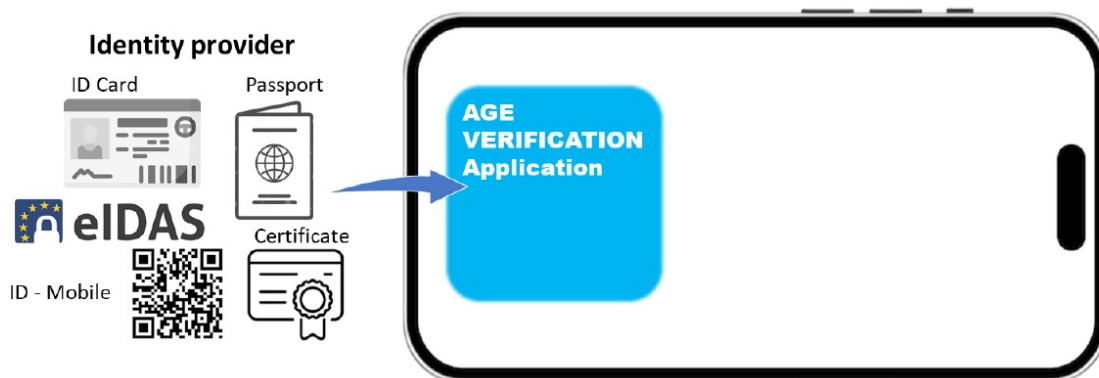


*Browser that receives labeled content, but does not display it if it requires age verification*

The age verification app acts as an intermediary between different identity providers and the application that needs to verify age to allow access to certain content (e.g. the browser 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.

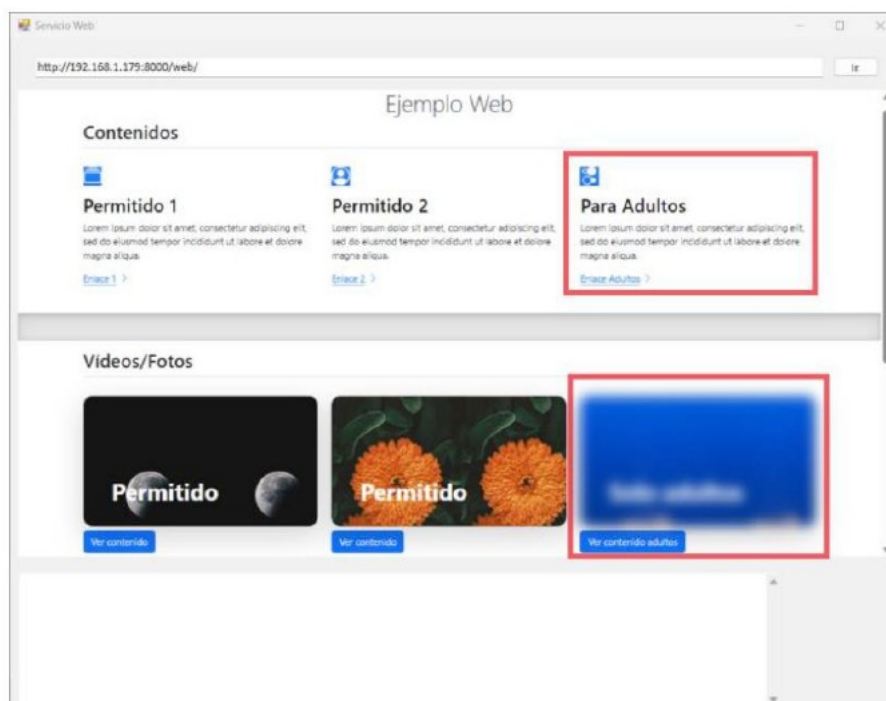
The age verification app, executed solely on the personal device and provided by an entity selected by the user, shall prevent the disclosure of identity. Positioned between the identity and the generation of the 'access authorised' condition, this app allows control so that the identity is never revealed to content providers or third parties.



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

Example of accessing content from your computer:

1. The user requests access to content labelled 'for adults' by the browser.
2. The content is received with its label, and the display of the content on the device is initially blocked (in the PoC, the content is shown as blurred). In this way, the status of a minor is not revealed to the content provider, and the content is always served.

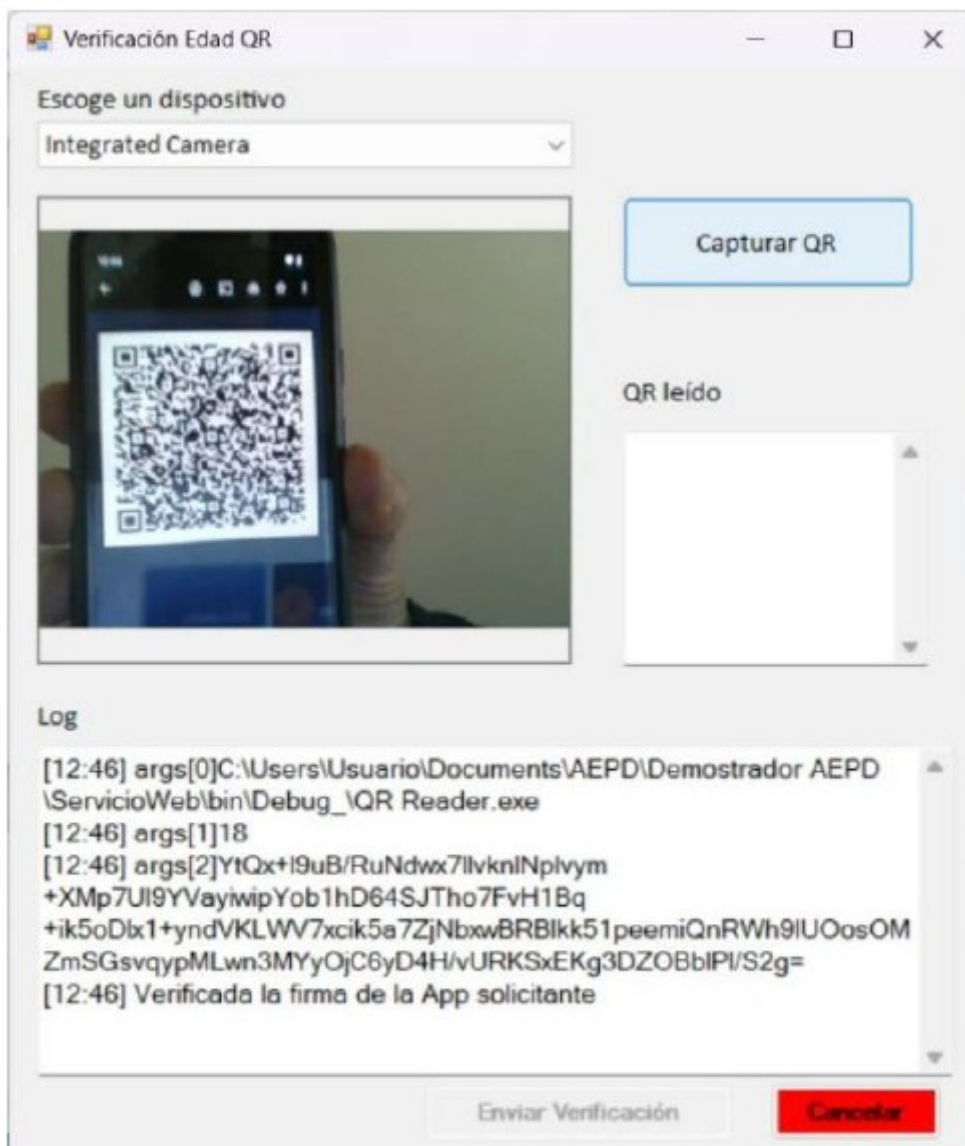


*Browser che riceve contenuti etichettati, ma non li visualizza se richiede la verifica dell'età*

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

*Browser that receives labelled content but does not display it if it requires age verification*

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



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

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

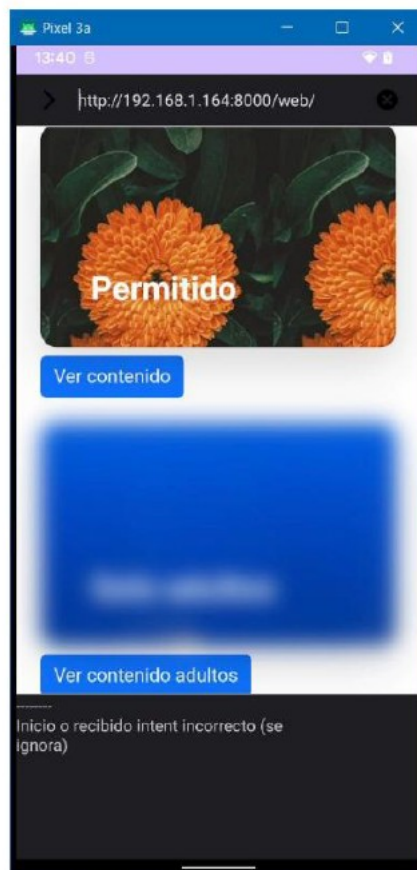
*Read and check the QR code in the age verification application*

3. Two different situations can occur:

- The age verification application responds with the condition ‘access authorised’, without revealing identity information. The browser removes the filter, and access to the content becomes totally unrestricted.
- The age verification application does not respond with the condition ‘access authorised’. In fact, it does not respond in any way, 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 the status of a minor is not revealed), or because the age verification application has not been installed, or because its use is not authorised, or the QR code is not available, or for any other circumstance.

**Use of mobile phone**

1. The user requests access to content labelled ‘for adults’ by the browser.
2. The content is received with its label, and the display of the content on the device is initially blocked (in the PoC, the content is shown as blurred). In this way, the status of a minor is not revealed to the content provider, and the content is always served.

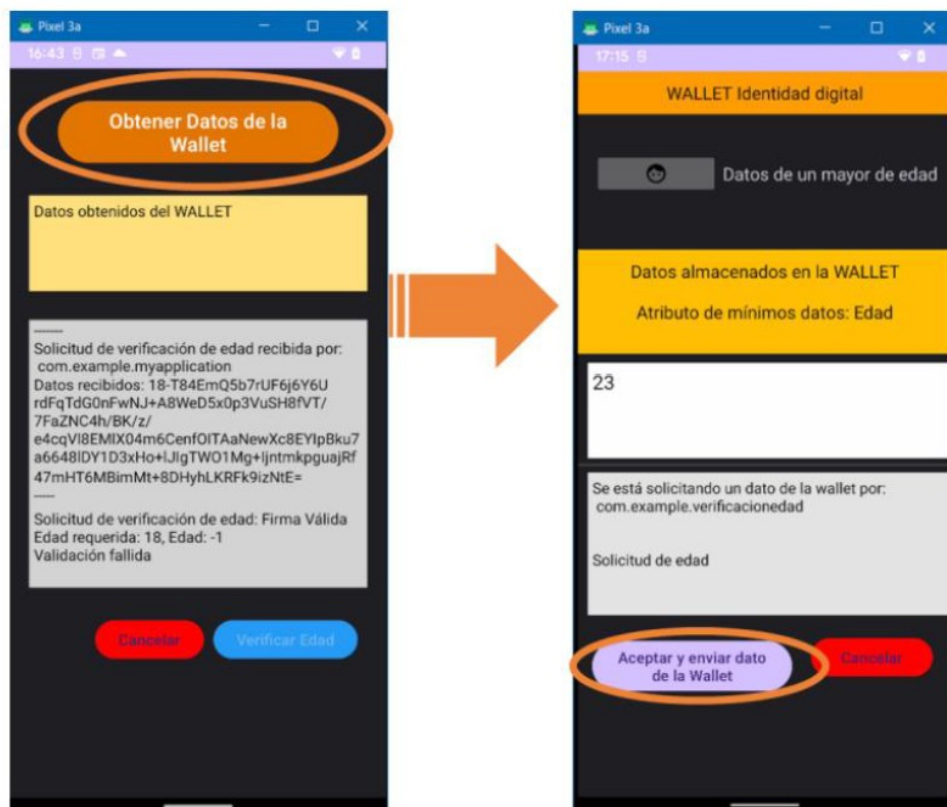


*Browser che riceve contenuti etichettati, ma non li visualizza se richiede la verifica dell'età*

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

*Browser that receives labelled content but does not display it if it requires age verification*

4. The browser queries the verification application to determine if the user is of the appropriate age to access the content (over 14 years old, over 18 years old or other conditions). The age verification application uses the information stored in the digital wallet to carry out the necessary checks.



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

<i>L'app di verifica dell'età riceve la richiesta dal browser e comunica con il portafoglio digitale</i>	<i>The age verification app receives the request from the browser and communicates with the digital wallet</i>
--	--

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

## 2.9 1.8 Observations on the use of public systems

As part of 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 envisaged in the opinion of the Commissioner, the following is stated.



The use of public databases or of an authentication system such as SPID could theoretically allow one to prove their age to access certain online sites or services. However, it is a system created to simplify access to PA services. Where its operation requires the registration of uses on the servers of State bodies and private companies, **it would have a list of connections of a purely private nature and presumed sexual orientations.**

By way of example, the SPID system, for example, does not appear, for the purposes of implementing the provisions of Article 13a of Law No 123 of 13 November 2023, to fully comply with the AGCOM's technical specifications indicated below (essentially in the part where so-called double anonymity is required), at the time of transferring to the Identity Provider the request for authentication from the Service Provider, which contains the domain name of the site visited. That SPID authentication system allows the Identity Provider to know the particular site/platform visited by the user and it is not excluded that this information is stored within the systems of the Identity Provider.

The method of authentication *SPID Single Sign On - SP initiated redirect* 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 the purposes of authentication, but through the *User\_agent*.

As shown in the *SPID Single Sign On* technical documentation, messages <sup>26</sup> containing metadata are exchanged from the *Service\_provider* to the *User\_agent* and from the *Identity\_provider* to the *User\_agent*.

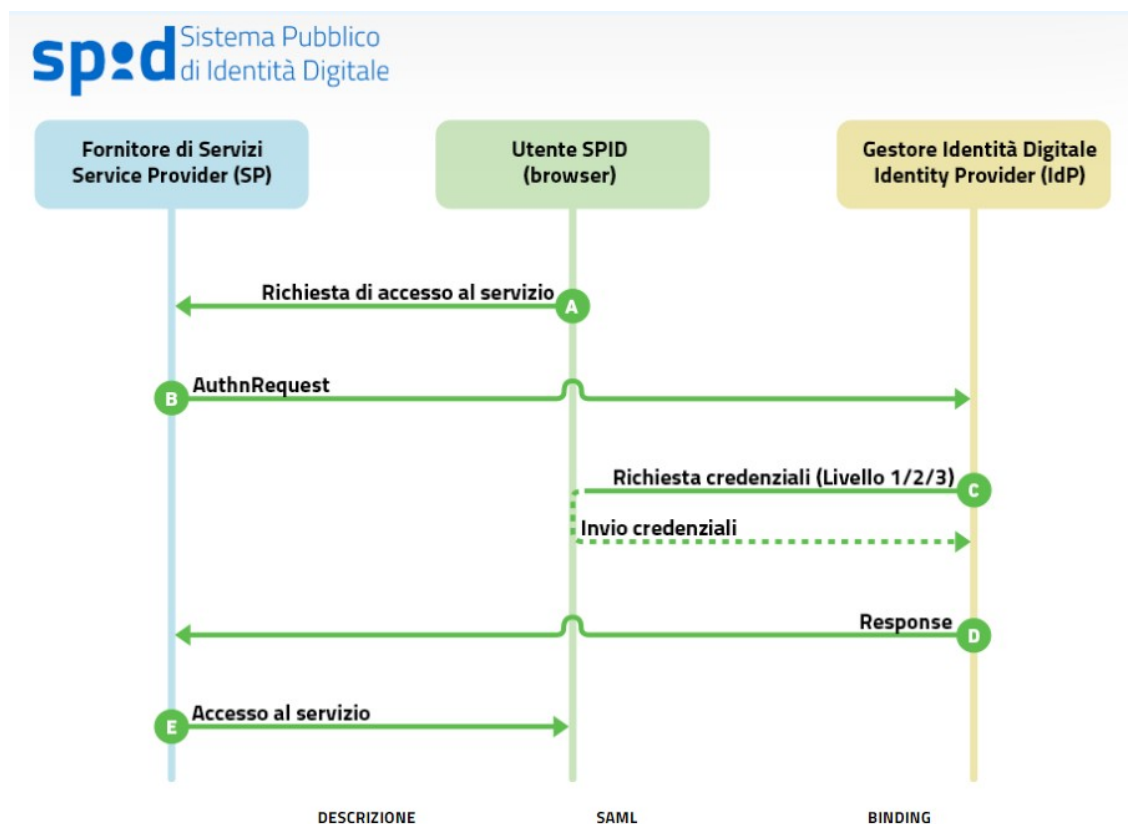
The authentication mechanism is triggered by the user's selection of the Identity Manager with which they intend to log in; this selection takes place on the Service Provider's website by means of an official 'Enter with SPID' button to be integrated into the service. The Service Provider shall accordingly prepare an **<AuthnRequest>** to be forwarded to the Identity Manager, where the user is redirected to authenticate. Once the authentication has been performed, 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, surname, tax code) that the Service Provider can use to authorise the user according to its own policy and provide the requested service.

Below is a diagram that represents the flow of the interactions described above.

---

<sup>26</sup> available at <https://docs.italia.it/italia/spid/spid-regole-tecniche/it/stabile/single-sign-on.html#esempio-di-authnrequest>





Fornitore di Servizi Service Provider (SP)	Service Provider (SP)
Utente SPID (browser)	SPID user (browser)
Gestore Identità Digitale Identity Provider (IdP)	Digital Identity Provider (IdP)
Richiesta di accesso al servizio	Request for access to the service
AuthnRequest	AuthnRequest
Richiesta credenziali (Livello 1/2/3)	Credential request (Level 1/2/3)
Invio credenziali	Sending credentials
Response	Response
Accesso al servizio	Access to the service
DESCRIZIONE	DESCRIPTION
SAME	SAME
BINDING	BINDING

The message **<AuthnRequest>** is therefore sent by the Service Provider, through the User Agent, to the *SingleSignOnService* of the Identity Provider to initiate the authentication flow. It may be forwarded by a Service Provider to the Identity Provider using the *HTTP-Redirect binding* or the *HTTP-POST binding*.

The documentation published by AGID shows that this **<AuthnRequest>** message contains the attribute **'AssertionConsumerServiceURL'**, which indicates the URL of the Service Provider, **i.e. the address of the website visited by the user**, to which the

response message to the authentication request should be sent (the address must match the address of the service indicated by the <AssertionConsumingService> element present in the Service Provider's metadata)<sup>27</sup>.

Therefore, that SPID authentication system allows the Identity Provider to know the particular site/platform visited by the user and it is not excluded that this information is stored within the systems of the Identity Provider.

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

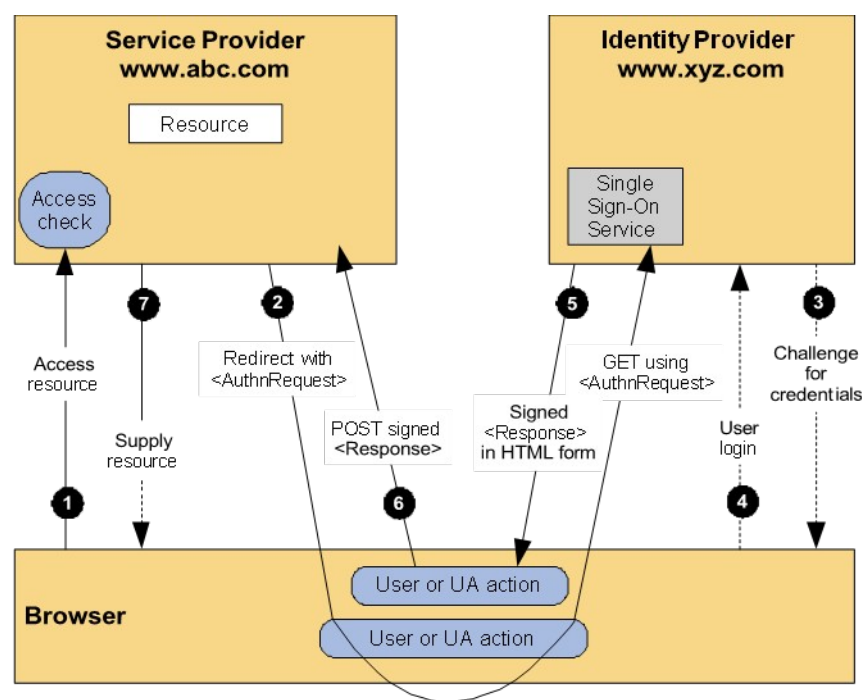


Figura 1 - SSO SP-Initiated Redirect/POST binding

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

<sup>27</sup> The response sent by the Identity Provider to the Service Provider can only be transmitted via the HTTP-POST binding and must contain, according to those specifications, the Destination attribute, indicating the URI reference of the Service Provider to whom the response is sent.

“2 A.		AuthnRequest	
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	The Identity Provider, upon successful authentication, performs the user login and prepares the assertion containing the user's authentication statement intended for the Service Provider (plus any attribute statements issued by the Identity Provider itself).	-	-
5	The Identity Provider returns to the User Agent the <Response> SAML containing the assertion prepared in the previous point.	Response	HTTP POST
6	The User Agent forwards to the Service Provider (SP) the <Response> SAML issued by the Identity Provider.	Response	HTTP POST

**Table 1 - SSO SP-Initiated Redirect/POST binding**

Please note that step 2b of the above table does not appear to comply with the AGCOM technical specifications (double anonymity) set out below when the request for authentication by the Service Provider, which contains the domain name of the site visited, is transferred to the Identity Provider.

The Authority, therefore, only if the requirements of the regulation in Annex A on double anonymity are met (protection of personal data against the site/platform and lack of knowledge of the site/platform visited by the Identity Provider), considers that public systems are usable.

## ANNEX C to Redolution No /24/CONS

### RESULTS OF THE PUBLIC CONSULTATION REFERRED TO IN RESOLUTION NO 61/24/CONS

#### Summary

<i>I. THE PROCEDURE.....</i>	<i>101</i>
<i>II. GENERAL CONSIDERATIONS.....</i>	<i>102</i>
<i>III. OBLIGATIONS AND SUBJECTIVE AND OBJECTIVE SCOPE OF THE GUIDELINES.....</i>	<i>106</i>
<i>IV. METHODS OF IMPLEMENTATION OF AGE ASSURANCE SYSTEMS.....</i>	<i>111</i>
<i>V. ON THE FREEDOM OF CHOICE OF AGE VERIFICATION SYSTEMS BY REGULATED ENTITIES.....</i>	<i>121</i>
<i>VI. ON ISSUES RELATING TO THE PROTECTION OF PERSONAL DATA.....</i>	<i>122</i>
<i>VII. ON THE INTERVENTION OF INDEPENDENT THIRD PARTIES.....</i>	<i>125</i>
<i>VIII. ON THE SECURITY OF SYSTEMS.....</i>	<i>129</i>
<i>IX. ON THE CRITERIA OF ACCURACY AND EFFECTIVENESS.....</i>	<i>131</i>
<i>X. ON THE CRITERIA OF ACCESSIBILITY, EASE OF USE AND NON- DISCRIMINATION.....</i>	<i>133</i>
<i>XI. ON THE TRANSPARENCY CRITERION.....</i>	<i>134</i>
<i>XII. ON TRAINING AND INFORMATION.....</i>	<i>135</i>

## ***I. THE PROCEDURE***

By Resolution No 61/24/CONS of 6 March 2024, the Authority launched the public consultation referred to in Article 1(4) of Decision 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 13 November 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<sup>28</sup> (hereinafter referred to as **WEBGROUP**), Aylo holdings<sup>29</sup> (hereinafter referred to as **AYLO**), [OMISSIS - an electronic communications operator (hereinafter referred to as **an operator**)], the Commissioner for Children and Adolescents (hereinafter referred to as **COMMISSIONERFOR CHILDREN**), the National Users' Council (hereinafter referred to as **CNU**), the Italian Parents' Movement (hereinafter referred to as **MOIGE**), Altroconsumo, Forum of Family Associations (hereinafter referred to as **FAF**)), the Centro Italiano Femminile (hereinafter referred to as **CIF**), the Movimento Cristiano Lavoratori (hereinafter referred to as **MCL**), Noi Trento APS (hereinafter referred to as **NOI TRENTO**).

Following receipt of the written contributions, the participants in the proceedings were heard in sessions held in May 2024.

The results of the public consultation are set out below.

---

<sup>28</sup> WebGroup Czech Republic, a.s. is a company, incorporated in the Czech Republic, which operates the XVideos website available at [www.xvideos.com](http://www.xvideos.com). XVideos hosts and makes adult videos available to users for free. Users can also create an account to upload their 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.

<sup>29</sup> Aylo Holding S.à.r.l. is a technology and media company, owning a broad portfolio of adult entertainment businesses (Pornhub, YouPorn, Redtube, Brazzers). The main activities consist of free and subscription video streaming sites. Aylo's main business units are as follows: video sharing platforms (VSPs), paid sites, model content platforms, advertising platforms and video game platforms.

## **II. GENERAL CONSIDERATIONS**

### **A. Observations of institutional bodies, operators and associations**

#### ***The need for effective age verification systems***

The **COMMISSIONER FOR CHILDREN** 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. This need is made all the more urgent by the growing and massive use of artificial intelligence, which is causing further transformations with results that are difficult to predict. He considers that, although appreciable progress has been made in introducing various tools and mechanisms to protect young users from the pitfalls of the network, many of these measures are still completely insufficient. He adds that it is evident that most age verification systems are still based on easily circumventable methods that involve 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 acknowledging that the problem is very complex and difficult to solve also due to the lack of consistent standardisation and regulation in the different countries, which can create disparities and gaps in protection systems, making it impracticable to adopt effective solutions on a global scale, the COMMISSIONER appreciates that the Authority has implemented a rule to which the legislator has given urgent importance and which aims to introduce an age verification system capable of preventing access by minors to pornographic image and video sharing sites and platforms.

The **CNU** appreciates Agcom's attention to protecting the rights and legitimate needs of minors as active participants in the communication process, as also provided for by 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 majority will help prevent the exposure of minors to content that is inappropriate for their age, content that can undermine their psycho-physical well-being. **It therefore states that the solution which the Authority has submitted for consultation, with the favourable opinion of the Privacy Commissioner, is fully endorsed by the CNU.** It also considers that it is necessary to define age verification

methods in such a way that they are clear, effective, and verifiable through a robust certification and interoperability framework, as the online age verification methods already on the global market most often entail privacy and IT security risks because they over-process personal data such as, for example, identity card data, credit card data, facial recognition, or analysis of the user's online behaviour. These methods require an excessive proliferation of sensitive data that is beyond the control of the data controllers and entails risks in terms of security and transparency. Other verification methods (e.g. self-declaration) are very ineffective as they can be easily circumvented, others are characterised by a high margin of statistical error and, in this case, the risk is that the child will be able to access harmful and inappropriate content, without limitations or controls.

The **MOIGE** highlights, in pursuit of the best interests of minors and in order to guarantee for them the maximum protection also on the internet, the legal importance of the problem of access for minors to social networking platforms and to all information society services, given that the use of these services is still the performance of a negotiation activity as it is subject to the conclusion of a contract and the related conditions of use of the services offered by the providers. It identifies, therefore, an opposition within the legal system in that the legislation allows minors, after the age of 14, to use electronic communications services, although to access social networking platforms it is necessary to sign actual contractual clauses, accept the terms of service, and give their consent to the processing of personal data for purposes inherent in the performance of the contract. In fact, to access the platforms of social network sites, it is necessary to sign the terms of use, which are actual contractual clauses, accept the terms of service, and give your consent to the processing of personal data for purposes related to the execution of the contract. It points out that, under Italian law, a minor cannot lawfully dispose of his or her rights and interests, e.g. property rights, since Italian law confers legal capacity on a person who has reached the age of majority. Yet, it adds, due to a sort of phenomenon of communicating vessels, the subjective condition for the provision of consent to the processing of personal data under EU Regulation 2016/679 has become *de facto*, not *de jure*, 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 children's personal data by means of the artifice of differentiating the age for accessing information society services from the age for carrying out any other legal activity is unlawful and in breach of mandatory rules of Italian law and of any legal system that requires, in order to acquire the capacity to act, the age of 18 years. Due to a sort of phenomenon of communicating vessels, the subjective condition for the provision of



consent to the processing of personal data pursuant to Article 6(1)(a) of Regulation (EU) 2016/679 has become *de facto*, even if not *de jure*, the subjective condition for the conclusion of a contract for the provision of services, given that the possibilities of 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 displaying content or activities not suitable for minors. Furthermore, it points out that, under Article 17 of Legislative Decree 70/2003 the information society service provider is not obliged to monitor the information it transmits or stores, so the civil liability for acts committed by the minor on the network lies with the persons exercising parental responsibility: This is why it is urgently necessary to restore to parents the real possibility of control and decision on the use by minor children of social networking platforms and to restore the age of eighteen to validly express any kind of will and consent, including for the provision of information society services. Finally, it requires the adoption of systems that, with the utmost effectiveness and security, guarantee a specific expression of consent on the part of those exercising parental responsibility for access to platforms that provide communication services or make audio and video content available.

**NOITRENTO** supports the need for genuine *age verification* for accessing sites that require users to be of majority age.

The **MCL** represents that the methods of online age verification used so far have not been able to protect minors from content that may damage and compromise their physical, mental, and moral development and well-being, and therefore considers it urgent to identify and activate new mechanisms that guarantee a high level of protection and, while respecting privacy, do not allow minors to access content and activities that irreparably damage their harmonious and integral development. It also calls for this public consultation not to be an episodic initiative, but to establish a constantly monitored and updated protection system capable of involving and supporting families.

The **CIF** confirms that it fully approves the measure governing the technical and procedural methods for ascertaining the age of majority of users.

**ALTROCONSUMO** considers it useful to add the definitions of ‘proof of age’ and ‘certifying entity’. It stresses that the principle of proportionality must serve as a counterbalance in the weighing of 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 caution, as it is better to ‘wrongly’ protect an adult than to

omit protection for a minor. For these eventualities, it proposes to provide for ‘correction’ systems *ex post* if the use of a site or content by an adult is blocked.

The **FAF**, in welcoming the opening of the public consultation on the technical and procedural methods that the persons identified by the legislation are required to adopt to verify the age of majority of users, considers it necessary to act on several fronts. In fact, in addition to the parental control filter set up by operators, it considers that sites that disseminate video material intended for an adult audience, such as Pornhub and many other similar sites, should also provide appropriate forms of age verification.

### ***On the need for a harmonised approach at European level***

**META**, while understanding that the aim of the law is to prevent access to pornographic content (thus not directly applicable to Meta), considers that access to content that is inappropriate or intended for an adult audience should be considered within a broader and more articulated framework; rather than aiming at the introduction of various *age assurance* methods adopted by different actors that, in addition to generating a fragmented and ineffective framework, could cause significant risks with respect to data minimisation. Furthermore, in order to ensure their effectiveness, it considers it necessary for these solutions to be discussed at European level, as well as at sector level. Similarly, it considers it essential that all apps are subject to the same standards to ensure a coherent and effective approach to protecting young people. Collaborating across the industry 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 safety and age-appropriate experiences. Finally, it considers that a multilevel approach should be adopted for age verification, including the possibility for users to choose an age assurance mechanism based on feasibility and preferences, so as to ensure fairness and objectivity of the process.

### **B. Assessments by the Authority**

**The Authority** acknowledges that both institutional and private entities recognize the necessity of an effective age verification system and that the solution proposed by the Authority is appropriate for balancing the requirements of effectiveness and personal data protection. It also considers it appropriate that the issue of access to content that is inappropriate or that is intended for an adult audience should be considered in an international or, at the very least, European context in order to avoid a fragmented reference framework and to ensure the effectiveness of the solutions. The Authority also

agrees on the necessity that all apps should be subject to the same minimum standards in order to ensure a coherent and effective approach to protecting young people. The Authority, therefore, with these technical specifications, adopts a *future-proof* approach, while simultaneously complying with the requirements of Decree-Law 123/2023 (as converted into law) and being able to incorporate future Community provisions on age verification systems and decisions to be made in this area.

### **III. OBLIGATIONS AND SUBJECTIVE AND OBJECTIVE SCOPE OF THE GUIDELINES**

#### **A. Observations of institutional bodies, operators and associations**

The **COMMISSIONER FOR CHILDREN** hopes that it will be possible to **extend this protection also to other content that is seriously harmful** to the physical and mental health of children and adolescents, such as content inciting hatred, violence, and other improper and harmful practices, even if not included in the purposes of the consultation.

**ALTROCONSUMO** considers that the **assurance systems outlined can be applied with reference to the contents subject to the parental controls referred to in Resolution 9/23/CONS**, which include, but are not limited to: adult content, gambling, betting, content related to weapons, drugs, violence, hatred and discrimination, promotion of practices that may harm health in the light of established medical knowledge, sects.

**META** recommends limiting the definitions set out in the text only to the entities defined by Article 13a of Decree-Law No. 123 of 15 September 2023. In particular, it considers that **the definitions of ‘regulated service’ and ‘regulated entity’ should include only services and entities that facilitate access to pornographic content**, as defined in Article 13a of Decree-Law No 123 of 15 September 2023, avoiding a general application to other types of services offering content reserved for adult users.

**AYLO** considers that the definitions **should include not only video sharing platforms, but all websites and social media that are also 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 happened in other jurisdictions, almost no user (regardless of age) would continue to visit that site, and users would simply switch to numerous other sites which do not require verification and age estimation systems, which would probably be less compliant with the law and subject to significantly lower reliability, security measures, and content moderation. Therefore, it considers that the effective protection of minors would be null, as users would simply move to less protected sites that do not comply with the law. Furthermore, it highlights that users who decide not to move to other sites would use other methods to circumvent the age protection requirements, regardless of the specific form adopted. On the subject, AYLO represents 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 that are most likely to comply with the law, as they are able to invest more resources in the processes of reliability and security and moderation, 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 so far done so in countries where regulation has been made), and this entails a substantial increase in the risk for users of being exposed to potentially harmful material on websites without adequate controls. For example, in the American states where AYLO has introduced age verification and age estimation or removed access to its platforms, there has been a surge in searches for other, often unregulated, adult sites with little or no 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 (USA) where, in 2023, following the adoption of a rule obliging websites/platforms providing pornographic content to carry out age verification using an electronic identity card, access to its platform decreased by 80% and, at the same time, searches for alternative sites, methods of circumvention of controls and use of VPNs increased.

In light of the above, it considers it essential that — in order to protect minors from content intended for adults online in the most comprehensive and effective way — the scope of these obligations should be sufficiently broad to include all such content.

**In conclusion, AYLO** considers that, to ensure that children are protected from online content intended for adults, the scope of the new legislation should be sufficiently broad to include all potentially harmful content, including social media websites that allow the use of adult material, stressing that a solution implemented at the device level would represent the best option to block other content that is not suitable for children.

**WEBGROUP** considers that in the event that 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 and, in particular, with the law of the country of origin**, as laid down in Directive 2000/31/EC of the European Parliament and of the Council of 8 June 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 respect 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]** considers that the **provision would not apply to [OMISSIS - a video sharing platform provider]** as a **provider established in a third country**, as well as due to the fact that the company does not allow users to disseminate pornographic content through its platforms; however, it agrees with the need to establish mechanisms to protect minors from content aimed at adults. It adds that the **development of a European framework for age assurance is the right way** and, therefore, these efforts should also be taken into account for the purposes of the measure under consultation.

**[OMISSIS - A video sharing platform provider]** considers that, in order to adequately protect children online, the age assurance tools must be: (i) proportionate; (ii) respectful of the rights to protection of personal data of the user and the user experience; and (iii) simple and effective. Agrees with the Authority that it is essential that any initiative adopted in this area is proportionate. As a result, the age assurance measures should restrict children's access to content without harming their personal data and fundamental rights through overly restrictive means of protection. In this context, it also considers it useful to note that **Article 28 of the DSA requires online platforms to take 'appropriate and proportionate' measures to ensure the protection of children online but does not impose any obligation to use age assurance tools - the adoption of which remains at the discretion of the providers**. Indeed, 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 considered each time. In that 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 for minors)**.

**[OMISSIS – An operator]** argues that the obligations and responsibilities for the implementation of the age verification methods will refer exclusively to the categories of subjects identified by the legislation, and not to those who do not offer content or video-sharing platforms, such as **providers of electronic communications services**. **It considers that the latter, having no connection with said services, must 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 that service and therefore to comply with age verification requests. In order not to impose an obligation on independent third parties that rests with websites and platforms, it considers that **the Operator must maintain discretion in the provision of such an Age Verification service to regulated entities**. In fact, it does not consider the requirement that the operator must comply with each request for age verification by the sites to be proportionate. It highlights that the exceptional number of requests that the entity responsible for technically carrying out the verification activity should process, and the necessary investments, especially in light of a possible expansion of the scope of the proposal for a regulation, cannot be disregarded.

## **B. Assessments by the Authority**

The Authority notes that the COMMISSIONER FOR CHILDREN hopes that it will be possible to extend the proposed age verification system for the protection of minors also to other content that is seriously harmful to the physical and mental health of children and adolescents, such as content inciting hatred, violence, and other improper and harmful practices, even if not included in the purposes of the consultation. In the same opinion, ALTROCONSUMO considers that the guarantee systems outlined can be applied with reference to the contents subject to parental control 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 include only services and entities that facilitate access to pornographic content**. WEBGROUP considers that in the event that 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 and, in particular, with the law of the country of origin**. Also, **[OMISSIS – A video sharing platform provider]** considers that the **rule would not apply to [OMISSIS – A video sharing platform provider]** as a **supplier established in a third country** and that the **development of a European framework for age assurance** is the right path to follow; where applicable, in line

**with Article 35(1)(j) of the DSA, the 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 for minors).**

With reference to the comments of META, AYLO, and WEBGROUP regarding the existence of the obligation and the subjective scope of application, the Authority, also considering the proposals of the CHILDREN'S OMBUDSMAN and the consumer association, deems it appropriate to clarify, in light of the observations from some parties involved in the public consultation, that the rules governing the technical and procedural methods for verifying the age of majority 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 the operators of websites and by the providers of video-sharing platforms that disseminate pornographic images and videos in Italy, wherever they are established.

On this point, the Authority considers that, in light of the regulatory framework referred to above and the comments made by participants, that the technical and procedural arrangements for verifying the age of majority of users approved by this measure are highly recommended, as they are effective, suitable, proportional, and functional, for their own use as well as by entities other than those directly regulated herein and with reference to other types of content, in addition to those of a pornographic nature, which could in any case harm the physical, mental, or moral development of minors, such as the categories provided for by Resolution 9/03/CONS.

In sharing AYLO's comment, the Authority considers it reasonable that the objective scope of the application should include not only video sharing platforms, but all websites and social media that are also capable of sharing sexually explicit content. With regard to the observation that it is likely that only providers of large sites and platforms will implement the measures in question, it is considered that adequate supervision, including through the cooperation system provided for in the Digital Services Act, and appropriate regulatory safeguards can act as a deterrent. Pursuant to the TUSMA, moreover, as explained below, the Authority may in any case inhibit the circulation of harmful content, disseminated by providers established in other States, to users located in Italy.

With reference to the observation of [OMISSIS – An operator], the Authority considers it reasonable, where private parties intervene as third parties, for owners of



video-sharing platforms and websites to interact with them through commercially negotiated agreements.

#### **IV. METHODS OF IMPLEMENTATION OF AGE ASSURANCE SYSTEMS**

##### **A. Observations of institutional bodies, operators and associations**

The **COMMISSIONER FOR CHILDREN** considers that, among the various solutions proposed in the consultation, in accordance with what has already been proposed in the context of the Technical Round Table on the protection of the rights of children online in the context of social networks, digital services and products established at the Ministry of Justice by Ministerial Decree of 21 June 2021, **the adoption of a system based on the use of a digital identity of type SPID ensures 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 protection of personal data and protection from content harmful to minors. This is in line with the European Commission's call for the new European Strategy for a Better Internet for Children (BIK+), adopted on 11 May 2022, which invited Member States to support effective age verification tools in line with the recently adopted European Digital Identity Regulation (EU Regulation of 26 March 2024). Moreover, while acknowledging that other solutions make it easier to achieve decent levels of protection, it considers that child protection cannot be limited to the use of systems already employed in the past, such as parental control, a tool which, although very flexible and adequate when activated to offer protection to children online, has seen limited adoption in both traditional and new media, due to low usage by responsible adults, often encountering certain difficulties in its application.

**WEBGROUP** stresses the importance of considering that age verification can be carried out more efficiently at the level of the user's device, for example in the form of filtering software (APPs), rather than at the website level. This gives users absolute control over their identity and age and minimises 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 the approval of a law in favour of age verification, to no longer implement age verification due to a detailed study that confirmed numerous problems with the technology connected to it. In particular, the Australian government is currently working with industry representatives to develop effective educational mechanisms for parents, so that they **use device-level filtering software to restrict children's access to harmful material**.

As a further example, it adds that **Spain has recently launched a pilot programme, developed by the National Agency for Data Protection (DPA), which plans to carry out age verification at device level**.

The solution provided by the Spanish DPA is based on **content labelling** (through tags) by online service providers, which allows content to be classified as sexual, violent and/or racist. The access restriction is carried out locally on the user's device instead of by the online service provider or even by third parties as intermediaries. The system is based on a virtual interaction that is established between the browser of the PC and an APP installed on the user's mobile phone. In this way, access to content reserved for adults through the browser of the PC is managed by an age verification app to be installed on users' mobile phones. The PC browser, after analysing the tags related to the web content, will require the user to verify their age — by scanning a QR code presented by the browser itself with their mobile phone — via the App installed on the mobile phone to grant or refuse access to specific content previously labeled by online sites and platforms as adult content or inappropriate content. On the other hand, eWallet solutions compatible with the eIDAS Regulation that work on 'age attribution' systems to provide confirmation of a specific age, while respecting the principle of data minimisation, apply to accessing content directly from a mobile phone. In this case, the mobile browser will request verification and interact with the eWallet App, also on the mobile phone, which provides the age of majority attribute.

**WEBGROUP** considers that **the solution envisaged by the Spanish DPA is suitable to balance the objectives of age verification systems** (i.e. preventing children's access to 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. In addition, it notes that minors are generally more at risk of being exposed to adult content from social media websites and search engines than traditional adult websites such as XVideos. It believes that search engines allow anyone to access a large amount of adult images and videos in seconds (content that is no less

explicit than that found on XVideos). For example, the association explains that Facebook reported as many as 73.3 million explicit contents such 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, or LinkedIn, not to mention much less popular but easily accessible websites. Finally, it reiterates that filtering software, or **device-level filtering software<sup>30</sup>, can be more effective in preventing children’s access to explicit content online and a wide range of adult content.**

**WEBGROUP** considers that, if the **age verification procedure is performed at the device level via software filtering**, without the intervention of a third party, the risk of a third party’s independence is eliminated. Furthermore, it considers that the introduction of a third party as the custodian of any information inevitably adds an additional level of concern regarding the protection of such data. Age verification conducted on the device adequately balances the interests of the child with the other rights of all Internet users, such as user anonymity. In this regard, it considers that **what is being implemented today by digital identity providers (such as the government authority issuing an electronic identity card or certificate) is sufficient, and there is no need to create any alternative digital identity system** for the purposes of age verification prior to access by minors to adult content.

**WEBGROUP** considers that an **age verification system at device level** would ensure that systems are fully verifiable and transparent, especially in light of the high risks that some existing age verification tools involve. In this regard, it should be noted that some of the most widespread age verification systems are made 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, puts their rights and freedoms at risk and is not effective in preventing children's access to adult content, thereby putting the privacy of site visitors at risk (for example, when identification information provided for age verification is revealed by hackers or otherwise). In addition, it considers that there is a risk that the entity carrying out the age verification may locate minors or collect their data. It believes that age verification entails the risk of blackmail for national security when access data is compromised. It adds that the age verification imposed on platforms is highly ineffective in light of a range of cheap and easily accessible technologies, such as virtual private networks (VPNs), as well as ineffective in geolocating individuals,

---

<sup>30</sup> ‘Filtering software’ generally means software installed on the device that can filter web pages/content for adults (at the level of a web browser as proposed by Spain, or even at the level of parental control application software).

with the result (especially close to national borders) that individuals are not subjected to age verification because the age verification provider wrongly 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 identity and the generation of the condition of authorised user, allows for age verification to be done without imposing verification on platforms, thereby avoiding all the risks associated with AV imposed on platforms. In the alternative, WEBGROUP believes that each provider should be free to choose the age verification mechanisms it considers suitable, and users should be free to choose the most convenient among the systems offered, without prejudice, in both cases, to the principles of effectiveness and compliance with the law. It considers that the Authority **should provide a list of controlled/certified AV service providers**.

**WEBGROUP** is also of the opinion that, from a proportionality point of view, it is reasonable **to make parents and tutors aware, in the first place, that the operating systems for the most popular computers, by Microsoft and Apple, directly include parental control functions 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 want 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 Qustodio, Kaspersky Safe Kids, FamilyKeeper, and others. These features allow parents to block access to sexually explicit material on the web, prevent minors from providing personal information to strangers via email or in chat rooms, limit children's viewing time, and keep a record of all online activities on a home computer. It 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 restrict and observe the use of the Internet by a minor, simply by placing a computer in a public space inside the house. All these methods are inexpensive (or free) and non-invasive (from the point of view of the principle of proportionality) to obtain effective age verification.

**WEBGROUP** considers that in the current state of technology, **facial recognition may not be technically safe or adequate**, as there is a large margin of error with regard to age and, in addition, the collection of biometric data also entails serious risks for the privacy of internet users.

**WEBGROUP** also considers it necessary to add definitions of 'parental control', 'filtering', and 'device-level age verification'.

**AYLO** considers that **the real solution to protect minors and adults is to verify the age of users at the access point — i.e. on users' devices<sup>31</sup> — at the operating system level** and to deny or allow access to age-restricted materials and websites based on such verification. This approach requires the **collaboration of operating system companies** and, with their consent, the transmission of personal data would be minimised, while protecting minors from harmful content. This would ensure greater ease of implementation, as operating system manufacturers are far fewer than websites/platforms that provide pornographic content. In addition, personal data would be better protected, as it would not be managed by a multitude of websites, and more effective protection would be ensured, since access for minors would be blocked to any pornographic content, including illegal or 'extreme' content, regardless of whether the websites/platforms implement protection measures. This solution could be implemented by ensuring that **operating system manufacturers block adult content by default**, so that minors are always protected when they access the internet, **and require age verification, at device level, only when the user requests access to adult content.**

**AYLO** points out that, when verification and age estimation are carried out on the device, users carry out such verification only once, through the operating system, and not on every age-restricted website. In this way, the risks of data theft and privacy are drastically reduced and a very simple process is created for regulators to control. In the opinion of **AYLO**, the technology to achieve this already exists today, in fact many devices already offer **free and easy parental control functions** that can be used to prevent children's accounts from accessing adult content without risking revealing sensitive user data. It adds that these features simply need to be improved to ensure proper verification or age estimation, and then be able to lock devices by default, unless they are unlocked after adult verification or age estimation on the device. Finally, it considers that the solutions implemented at device level would be the most effective from the point of view of functionality, ease of use and absence of impediments to use, as they would remain limited to the device environment, which is chosen and set according to the needs of the user, moreover in a well-known digital environment.

---

<sup>31</sup> By device-based age verification, **AYLO** means any approach to verifying and estimating age where personal information used to verify the user's age is shared in person with an authorized reseller, entered locally on the user's device, or stored on a network controlled by the device manufacturer or the device operating system provider. Through pre-installed content blocking and filtering software, which disables web browsing permissions or other means, the user cannot access content prohibited for their age on the Internet, unless they have been verified as having an age equal to or greater than the required age. To achieve this, this approach requires the collaboration of developers and operating system vendors.

**AYLO** argues that while an approach of implementing age verification at 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 meet 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 consider the methods of verification and age estimation at website level to be 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 easily access adult material online, because compliance with these requirements is only met by one or a few adult platforms and their implementation is poor. In light of the above, **it considers that the only effective solution to prevent children from accessing adult content is device-level age verification via the operating system,** where the default setting for all accounts and devices in the operating system is blocked adult content.

**AYLO** argues that it is difficult to consider any age assurance mechanism implemented at the website/platform level to be proportionate, except for the self-declaration method. It believes that the age assurance systems at website level other than self-declarations do not represent proportionate measures in light of the amount of risks they create and the harm they cause both to affected users 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, the risk is that any individual, including a minor, will be pushed to non-compliant sites (i.e. which decide not to implement such verification), and it is very likely that the user, even a minor, will thus be exposed to illegal and 'extreme' content with which, otherwise, they would never have come into contact. Therefore, the negative social consequences of adopting such a measure would be significant and completely unacceptable, **while being totally avoidable through the implementation of device-level controls.** It considers that the 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 the age verification and estimation systems at website level are also disproportionate in view of the economic rights and freedoms of platforms. In fact, it believes that any request to implement an identity certification requirement on their platforms would inevitably lead to an almost total loss of visitors to the platforms themselves, who would simply switch to doing something else and, consequently, the very existence of the platforms would be put at risk, since they would have almost no chance of surviving the total loss of traffic on them.



**META** is of the opinion that a significant step can be taken at European level to ensure that parents only have to verify the age of their child once and that the child subsequently has access to an age-appropriate experience in each individual app. **It considers that** instead of obliging parents to keep track of the many existing applications and all those that will be developed in the coming years, **it should be possible to verify age directly in the (virtual) place where adolescents download the application itself (at the app store or operating system level)**. According to the operator, this approach would reduce the burden for parents to identify the multiple apps used by their children and juggle the different age verification systems, and minimise the number of times and (virtual) spaces where they have to share potentially sensitive data to verify age. In addition, parents and adolescents would not be forced to provide their identity documents to all the applications in circulation to verify their own age or that of their children. Moreover, it points out that adolescents and parents already provide **app store operators** with this information when purchasing devices and creating accounts, which they have already integrated into their app store notification, review and approval systems that could be used directly by parents. **Therefore, it considers that verifying the age of an adolescent at the app store level ensure that apps downloaded from the app store meet the same standards of protection and provide age-appropriate content and experiences accordingly**. At the same time, a healthier and more competitive market would also be fostered, as the obligation to verify the 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 on the market. Finally, it believes that facilitating age verification for new apps targeting teens would not only foster competition, but provide parents with greater assurance that all apps, even those they've never heard of, comply with regulatory obligations.

**[OMISSIS – An operator]** considers 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, it cannot in any way be held liable if the adult does not take action to protect the child from access to sensitive content or if a minor actively decides to circumvent the security mechanisms put in place to protect him or her. One solution could be to verify age using contractual information associated with the IP address used by the user. That solution would make it possible to link the IP address used by the user while browsing with the contractual information of the SIM card holder available to the Operator. Verification by IP address requires a necessary distinction to be made between browsing by the user via a mobile



network or a fixed network. In the case of mobile browsing, it would be possible to compare the user's dynamic IP address with the contractual information available to the Operator only for a subset of users requiring proof of age by the mobile network. Indeed, **for the purposes of age verification, the Operator would be able to determine with certainty whether the user is a minor only in the case of a user using a 'Junior' SIM card in their own name.** In this case, [OMISSIS – An operator] explains that the dynamic IP used by the Junior user (holder of a 'Junior SIM') to browse using the mobile network would be associated by the Operator with the SIM of a minor, resulting in a KO on proof of age. On the contrary, if the dynamic IP were to be associated with a SIM card registered in the name of an adult (e.g. in the case of the father who names the SIM card and makes the minor child use it or in the case of an adult user), the Operator would approve **the proof of age on the basis of the age of the SIM holder, but without being certain that the real user of the SIM 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 using the IP address of the fixed network (e.g. via Wi-Fi or via Ethernet cable). This is because all fixed network contracts are by definition in the name of customers of legal age. Another possibility, explains the operator, is verification through 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). The verification through Parental Control would take place through querying the internal databases of [OMISSIS – An operator], i.e. whether or not Parental Control is active on the numbering that requires access. However, in line with what has already been stated above, even the case of using Parental Control as an age verification mechanism requires a distinction to be made between mobile and landline navigation, as the system is activated directly on the SIM. In the case of browsing on a mobile network with a Junior SIM, Parental Control is pre-activated by default and therefore the underage user is always protected, as this mechanism prevents access to the platforms under consideration. In the case of a non-Junior SIM card, the parent of the minor will be responsible for activating Parental Control on the minor's device. Therefore, age verification by means of Parental Control would be effective only in the case of minor users who are holders of a Junior SIM card, for which 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 active Parental Control — is actually an adult or a minor. On the other hand, it points out that in the case of fixed network navigation, since all fixed network users are adults, the parent of the minor would be responsible for activating the Parental Control mechanisms on the fixed network and, therefore, the minor user would be automatically blocked access to pornographic

content platforms in all cases in which Parental Control is activated on the fixed network by the holder of the contract. On the contrary, the minor would be granted access to the site/platform in all cases where the holder of the fixed network (over 18) does not activate Parental Control on the fixed network. In addition, it points out that the operator would not be able to verify the age of the user and to distinguish between an adult or minor user who relies on the fixed network (via Wi-Fi or via Ethernet cable).

### **B. Assessments by the Authority**

**The Authority takes note of the proposal of the COMMISSIONER FOR CHILDREN where it considers that the adoption of a system based on the use of a SPID digital identity allows to ensure a high degree of certainty in determining the age of the user and, at the same time, in compliance with the principle of proportionality.** Such a solution could be appropriate where providers provide an additional ‘proof of age’ function ensuring anonymity with respect to websites and platforms to which the user needs access.

It is also noted that the private associations and providers, WEBGROUP, AYLO, META, consider that **age verification should be carried out more efficiently at the user’s device level, e.g. in the form of filtering software (APP), rather than at the website level (e.g. the Spanish case). In other cases it is proposed to verify the age on users’ devices at the operating system level**, although it is recognized that this approach requires the **collaboration of operating system companies. One respondent in particular considers that age verification should be able to be carried out directly at the (virtual) place where adolescents download the application itself (at the app store or operating system level).**

In this regard, from a legal point of view, the Authority notes that the regulatory framework on age verification systems, and most recently Decree-Law 123/2023 itself as converted into law, does not impose an obligation on providers of terminals, APP stores, operating systems or browsers, but on providers of websites and video sharing platforms. With reference to the data security risks raised by WEBGROUP, the Authority notes that the approach proposed in the public consultation does not provide for any transfer of personal and sensitive information to the website or platform. The age verification is, in fact, done by the certified entity that is already in possession of the user’s data (independent third party model).

With reference to the observation that it would be sufficient to rely on the parental control systems provided for by the terminal operating systems, the Authority refers to the provisions of Resolution No 9/23/CONS as well as Article 13 of Decree-Law No 123 of 2023 as converted into law. At a general level, there is already an obligation for providers of electronic communications services and for terminal providers to implement a parental control system. However, the legislature has nevertheless decided to provide for an age verification system implemented by providers of websites and video-sharing platforms, inter alia, 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 labelling of site content to be interesting, not excluding that they may contribute to creating, in the future, an online environment that is safe for minors. The Authority considers it appropriate, in this regard, to set up a technical round table to monitor technical solutions, with the collaboration of all the institutional and private entities potentially involved. This provision, however, must be anchored to the current legal provisions that impose protection obligations on website providers and video sharing platforms with the caution of setting a discipline that is proportional and respectful of users' personal data.

**The Authority therefore confirms the provision of an age verification system implemented by the video sharing platform or website operator on the basis of the model proposed in consultation in which the transfer of user data to the platform or site visited is excluded.**

With reference to the request of some respondents who consider that the Authority should provide a list of audited/certified AV service providers please note the following.

**The Authority considers it appropriate to point out that any website or platform that falls within the subjective and objective scope of this measure, or that in any case voluntarily decides to apply these technical specifications (as better clarified in the section on the scope), must identify the entity that is able to provide proof of age in a certified manner in compliance with the legal requirements.**

**For the purposes of supervision, the Authority considers it appropriate to follow an approach similar to that used by Resolution No 9/23/CONS, in this case with**

reference to companies that are 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 13a of Decree-Law 123/2023, as amended when converted into law, must notify the Authority of the third parties entrusted with the activity of age verification together with a detailed report containing a description of the competences, the methods of age verification used and the reasons for the choice.

## ***V. ON THE FREEDOM OF CHOICE OF AGE VERIFICATION SYSTEMS BY REGULATED ENTITIES***

### **A. Observations of institutional bodies, operators and associations**

The CNU welcomes the fact that it is the entity required by law to choose the age verification tools to be implemented on its service, using a non-invasive tool as far as possible to achieve the desired objective, and to demonstrate the effectiveness of the tool used according to 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 range of **a maximum three verification systems** previously selected by it on the basis of the principles and requirements laid down, as leaving the choice between such dissimilar systems and processes — involving a difference in level in terms of safety and safeguards — to the full discretion of the parties concerned would lead to unreliable results and unequal treatment of users.

**[OMISSIS – An operator]** agrees that it should be up to the regulated entities to choose which Age Verification method must be implemented, provided that downstream of the present procedure, **however, a set of different procedures considered compatible with the principles and requirements established by the Authority is still provided for.** It is the opinion of the operator that **the Authority should provide regulated entities with a ‘range’ of age verification options, leaving it to the individual site/platform to choose which Age Assurance service to use**

**from time to time, on the basis of specific contractual agreements with the relevant providers.**

### **B. Assessments by the Authority**

The Authority takes note of the respondents' agreement with the approach proposed in consultation whereby it remains up to the provider of video sharing platforms and websites to select the appropriate age verification system that is, in any case, compliant with the provisions provided in this measure.

However, the Authority does not consider it appropriate to indicate a limited list of systems considered mandatory as, at present, it could represent a measure that is not proportionate and does not comply with the general principles of technological neutrality and freedom to conduct a business.

## **VI. ON ISSUES RELATING TO THE PROTECTION OF PERSONAL DATA**

### **A. Observations of institutional bodies, operators and associations**

AYLO highlights that Article 9(1) of the GDPR treats all personal data relating to the sexual orientation of a data subject as a special category of personal data and that these personal data are particularly sensitive. As such, they enjoy special protection under the GDPR, i.e. the requirement that data must be limited to what is necessary must therefore be of significant value in the case of processing of sensitive personal data. It considers that given the absolute lack of proven benefits in relation to the use of rigid identity certification/age-gating systems at website level, **it is neither appropriate nor relevant or supported by a principle of necessity within the meaning of Article 5 of the GDPR, to assume that one can collect and store users' personal data 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 the specific case are highly sensitive**, as they refer to the consumption of sexually explicit content by an individual. If such data became public, this could have significant consequences on their family, social and professional lives. Identity certification schemes can substantially harm the right of website users to self-determination with respect to their data. The data collected through these systems significantly increase the risk of hacking of such data. In addition, the risk of hacking

identity certification schemes particularly affects vulnerable groups such as the LGBT+ community. Furthermore, the standardisation of the practice of **uploading personal data to access websites carries significant risks, as it can lead to privacy breaches, identity theft and unauthorised use of sensitive data, highlighting the importance of safeguarding personal data in the digital age.** The attribution of this responsibility to the platform or platforms visited by a user implies that users repeatedly send private information to access different adult sites, normalising the disclosure of personal data on the Internet and creating a potentially irreparable risk of data identity theft globally. **With regard to privacy issues, it believes that operating systems today offer users the ability to limit the collection of browsing history and other data, providing a level of privacy protection managed directly by the user.** This autonomy is absent in age verification systems at the website level, which often operate with non-transparent data retention and use policies. In conclusion, it considers that **age verification systems implemented at the device level and those of age estimation would offer a more secure and privacy-friendly method, aligning with the principle of data minimisation and giving users more control over their personal information.**

**WEBGROUP** considers that to date there is no age verification system proposed that can guarantee the protection of users' privacy. Identity sharing for the purpose of accessing an adult site inevitably causes the identity of any user to be linked to their presumed sexual orientation or preference, which is the quintessence of the privacy breach and which exposes them to high risks, including national security. It argues, however, that **device-level user verification using filtering software avoids such problems because it minimises the amount of data shared** and does not associate it with the individual's access to pornographic websites and that no data other than what is normally collected to set up a device is collected. In addition, such data is not stored or shared online, but stored locally on the device, maintaining optimal privacy. Irrespective of the method of implementation, age verification — either through (i) the direct collection of identity documents by the publisher of the pornographic site; (ii) the estimation of age based on the browsing history of the Internet user; (iii) the processing of biometric data for the purpose of identifying or authenticating a natural person (for example, 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 SPIDs, provided in the public domain** — represents a **violation of privacy** where technology is limited and not advanced enough to protect and preserve fundamental rights. In fact, requiring websites to engage in AV or to use third-party AV providers creates highly sensitive and personally identifiable information stores, which are lucrative targets for hackers. **In this regard, it points out that AV double**

**anonymity mechanisms are an interesting but not yet mature option** and that, once properly developed and tested, the authorities should create certifications to screen the most secure/efficient service providers, not in a single country or a selection of countries, but in a coordinated manner and at least across the European Union.

**ALTROCONSUMO** considers that some age verification systems, including those involving the direct collection of documents or the processing of biometric data, must be excluded. There is no particular problem with the use of digital identities such as SPID as this is a proven and protected recognition and verification system. As regards age estimation based on browsing history, it considers that the subject called upon to verify their age would find themselves using personal data that are already potentially processed in the profiling operations carried out by the subject itself or by third parties, so they do not see any particular criticality in the use of the tool itself but consider it essential to prepare pseudonymisation measures that do not make it possible to trace the identity of the child but only to detect statistically recurrent elements in the navigation of minors.

## **B. Assessments by the Authority**

The Authority notes that **some respondents, representing providers of video sharing platforms and websites, consider that uploading personal data to access these platforms and websites poses significant risks, as it can lead to privacy breaches, identity theft and unauthorised use of sensitive data.** Therefore, they consider that **age verification systems implemented at device level** offer a more secure and privacy-friendly method, aligning with the principle of data minimisation and giving users more control over their personal information.

**In this regard, these respondents consider that AV double anonymity mechanisms are an interesting but not yet mature option** and that, once properly developed and tested, the authorities should create certifications to screen the most secure/efficient service providers, not in a single country or a selection of countries, but in a coordinated manner and at least across the European Union.

**A consumer association does not see any particular problems with the use of digital identities such as SPID** as this is a proven and protected recognition and verification system.

The Authority shares the view of the respondents that it is not **adequate, pursuant to Article 5 of the GDPR, to assume that it is possible to collect and store users'**



**personal data whenever a platform or website with adult content is visited and this is all the more true in light of the fact that the data processed in the specific case is highly sensitive.** In this regard, the Authority, precisely because of the risks for the protection of personal data highlighted, considers it appropriate to confirm the adoption of a system based on age verification by an independent certified entity without the transfer of personal data to the content provider.

As mentioned above, the interest in systems based on age verification and filtering at device level remains unaffected, even though these systems fall outside the scope of this measure, which lays down the process and system specifications that remain in the hands of providers of video-sharing platforms and websites that disseminate pornographic content.

It should be reiterated that the SPID system, does not appear, for the purposes of implementing the provisions of Article 13a of Law No 123 of 13 November 2023, to fully comply with the AGCOM's technical specifications indicated below (essentially in the part where so-called double anonymity is required), at the time of transferring to the Identity Provider the request for authentication from the Service Provider, which contains the domain name of the site visited. Therefore, as explained in Annexes A and B, appropriate adjustments should be made.

In this regard, the Authority considers it appropriate to include, among the systems suitable for the purpose of age assurance, 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 task force of the European Commission and at the same time meet the requirements of privacy protection, not providing for any upload of user data to the site or platform visited, and harmonisation of the 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 age) to be shared with the platform/site as part of the digital identity information. This solution is considered to address the concerns raised by institutional and private respondents.

## **VII. ON THE INTERVENTION OF INDEPENDENT THIRD PARTIES**

### **A. Observations of institutional bodies, operators and associations**

The COMMISSIONER FOR CHILDREN believes that the use of third parties, compared to those who manage the sites and online platforms, entrusted with the task of ascertaining the age of users and issuing a subsequent certified digital

**identity, offers several significant advantages.** He believes that this approach contributes to ensuring a higher level of impartiality and reliability in the age verification process as entities outside and independent of online platforms can operate with a higher degree of transparency and objectivity, minimising the risk of conflicts of interest or manipulation. Moreover, as specialised entities, they can be subject to strict data protection rules and regulations and, at the same time, foster greater consistency and uniformity in the age verification process across different online platforms and services. This can help ensure that children are protected in a uniform and consistent manner in any area of the digital world.

The **CNU** considers it **fully consistent with the objectives of proportionality, protection of personal data and security, to assign to independent third parties** (whether they are service providers specialising in the provision of digital identity or an organisation that has identified the internet user in another context such as a bank, a public administration, etc.) the issuance of a certified ‘proof of age’. It is therefore appropriate that it is not directly the sites and platforms subject to the age verification obligation that carry out the verification operations themselves. He considers that once the certified proof of age has been issued, it should be provided to the user so that he or she has access to the content requested on the site or platform visited. He stresses the appropriateness and risk minimisation of this method of ascertaining the age of users, as 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 acquire proof of age without becoming aware of the user’s identity as there will be no transmission of user identification data. The CNU also stresses the sensitivity of the further step through which sites and platforms interact with the independent third party, since it is desirable for content providers to equip themselves with clear and suitable tools aimed at acquiring and implementing the age verification system, in order to decipher the signature and establish its authenticity.

The **FAF** considers that the most common objection to the adoption of age verification systems is the breach of privacy of those who connect, who would be obliged to communicate their personal data contained in an identity document. To overcome this problem, **the viable solution is to use a third party** that protects such data (based on the model of the SPID). It points out that this is certainly a more demanding scenario in technological terms, and also in economic terms, but if it were the only way to bring all the actors involved together, it should certainly be promoted.

**ALTROCONSUMO stresses 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; the digital signature, the certified e-mail address so that each user can choose which person to contact to obtain the ‘proof of age’. It therefore suggests adding the ‘proof of age’ service to those already provided by digital identity. digital signature and certified e-mail address providers** from the moment when the user of one or more of these services has already been identified, and the ‘proof of age’ can be issued automatically in the personal area.

**[OMISSIS – An operator] agrees that a principle of provider independence should be used, as this mechanism also responds** to the requirements of the GDPR, minimising the amount of data retained by sites/platforms offering pornographic content and preventing the independent third party from becoming aware of the site/service to which the user wants 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 overturn the obligation on electronic communications operators to ensure the protection of underage users. **Therefore, it is willing to take on 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 must be offered on a voluntary basis and only against an economic remuneration by regulated entities.** Finally, it considers it necessary to impose a technical period of at least 12 months to allow 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 if TLC Operators were to be identified as independent third parties who decide at their discretion to offer these Age Verification services, it is immediately specified by the sector legislation that the necessary Age Verification activities are adequately and systematically remunerated by regulated entities, on the basis of trade agreements. In fact, it would be paradoxical that in the face of an obligation on the part of the regulated entities, the costs/investments by the suppliers of the related technical solutions to meet the aforementioned obligations were borne by the latter. In fact, at a technical level, the Operator should in fact have a system that is currently unavailable — which will require the support of investments as well as recurring costs — to process each request from regulated entities. It submits that service is to be regarded, for the independent third party, as a commercial service, which the operator is free to choose whether to offer on the market on the basis of commercial

agreements with regulated entities in light of a regulatory provision requiring payment of economic compensation.

**AYLO** represents that it is not able to evaluate the activities of third-party providers, however, it believes that the issues related to the age verification or estimation systems implemented at the website level are the same, regardless of whether their operation is borne by the platform or by a third-party provider. Those third parties, just like the platform, are obliged to carry out disproportionate data processing activities. It argues that, for the same reasons linked to the sensitivity of the information collected, this type of service could not even reasonably be delegated to third parties controlled by public bodies or otherwise subject to public authorisation. **Nevertheless, it still considers it necessary to involve third parties that develop operating systems ('OSSs').**

#### **B. Assessments by the Authority**

The Authority takes note of the general endorsement by institutional respondents and operators of 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 e-mail address providers** from the moment when the user of one or more of these services has already been identified, and the 'proof of age' can be issued automatically in the personal area.

We do not agree with the comment of the representative of platform providers/sites which considers that the issues related to age verification or estimation implemented at platform/website level are the same, regardless of whether their operation is borne by the platform/site or by a third-party provider. Those third parties, just like the platform/site, are obliged to carry out disproportionate data processing activities. In fact, the Authority has clarified that the third party is normally already in possession of user data for all the purposes laid down by law. This would include, among the digital identity information, the age attribute to be shared when accessing the platform/site.

In light of the favourable 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 providers of digital identity systems.

The Authority agrees, as already mentioned, that the intervention as a third party of a private entity, such as an electronic communications operator, must take place on the

basis of the offer of services subject to commercial negotiation, since phone operators are not subject to the legal obligation of age verification.

**In the context of an architecture based on a third party, the Authority considers it acceptable that, among the possible options, there is the option of adding the ‘proof of age’ service to those already provided by digital identity, digital signature and certified e-mail address providers** from the moment when the user of one or more of these services has already been identified, and the ‘proof of age’ can be issued automatically in the personal area.

**Having regard to the request to provide for a 12-month implementation period, the Authority points out that the time allowed for the implementation of the systems referred to in this provision is laid down in Article 13a(4).**

## **VIII. ON THE SECURITY OF SYSTEMS**

### **A. Observations of institutional bodies, operators and associations**

**META** believes that industry-wide collaboration 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 safety and age-appropriate experiences.

**AYLO** believes that age verification and age estimation systems at website level would result in significant harm, a breach of data protection principles and a huge risk to the right to self-determination of website users, creating unnecessary hacking risks for the large amount of highly sensitive personal data of users that should be collected. It highlights that personal data is attractive to attackers, so the risks of phishing attacks, identity theft, data breach and fraud increase as users share their information with an increasing number of websites and online age verification and estimation service providers. **It stresses once again that the best solution for mitigating security risks and circumvention methods in age assurance systems is the adoption of a device-level method.** This means that users would only be verified once, through their operating system, and not on every age-restricted website. This would drastically reduce privacy risks and create a very simple process for regulators to apply and for users to follow: More than 95% of devices worldwide are powered by operating systems owned by three companies. **AYLO** states that once verification and age estimation would first be performed on the device by operating system developers and device manufacturers, who already hold their users’ personal data, the latter would not be encouraged to

repeatedly share their personally identifiable information on the various sites. **In addition, the verification mechanisms implemented at the device level can offer greater security and reduce the risk of unauthorised access or data breach.** By locating age verification within the device, the treatment is isolated from the myriad vulnerabilities associated with online platforms, including hacking and phishing attempts. Finally, it believes that with a solution implemented at the device level, there would not even be the risk of a diversion of Internet traffic, i.e. the risk that users who do not want to reveal their personal information to access a website move from the compliant sites to the less secure and non-compliant ones.

**WEBGROUP** believes that **any age verification solution at device level is more secure than systems made by third parties.** In addition, 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, and is also likely to induce users, including minors, to venture into unregulated parts of the web, including the dark web, risk exposing themselves to more extreme explicit content, including criminal content, and cause much more serious problems than those that age verification imposes on the platforms. Furthermore, it believes that only when a new user accesses a personal device should age verification be required. Additional verification may also be required when internet browsing data indicates that the device is being used by a person other than the owner, or in the event of suspected identity theft or misuse.

It also argues that one of the negative aspects of the 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. Age verification **at device level** takes place on the user's device, regardless of the geographical origin of the website or its adult content, which also concerns the use of VPNs and **circumvention is much harder with verification systems limited to the user's terminal.**

**ALTROCONSUMO** considers that the self-declaration method is insufficient to certify the age of the user for obvious reasons, also confirmed by the elusive practices recorded in the use of some social platforms by young people (e.g. TikTok). In addition, if the age assurance system provided for an age check based on estimation, it is necessary to set up a double check mechanism by the site/platform by requesting documentary evidence. It stresses that this kind of mechanism must be accompanied by the due protections and responsibilities on the processing of personal data. With regard to the frequency of age verification, it considers that, **if the certification function were entrusted to the providers of digital identity, digital signature and certified e-mail addresses, a request system could be set up for each access.**

## **B. Assessments by the Authority**

**The Authority notes that the providers of platforms and websites that responded on the issue of security consider that the best solution to mitigate security risks and circumvention methods in age assurance systems is the adoption of a method at device level. In addition, the verification mechanisms implemented at the device level can offer greater security and reduce the risk of unauthorised access or data breach.**

They themselves observe that age verification **at device level** takes place on the user's device, regardless of the geographical origin of the website/platform or its adult content, which also concerns the use of VPNs and **circumvention is much harder with verification systems limited to the user's terminal.**

**The consumers' association considers that, if the certification function were entrusted to the providers of digital identity, digital signature and certified e-mail addresses, a request system could be set up for each access.**

**The Authority shares the concerns of respondents belonging to the category of providers of platforms and websites regarding the data security risks related to the possibility of sharing such information over the internet. As mentioned above, terminal-level verification solutions appear attractive but fall outside the scope of the present procedure concerning providers of video-sharing platform services and websites.**

With regard to the issue of security, the Authority considers that the system adopted by this measure, which could, *inter alia*, be based on a public and private key encryption system or in any case on secure connections, provides ample guarantees, although no one can exclude, in the IT sector, the possibility of circumvention of the solutions identified. Models based on digital identity, such as the ID Wallet, are also characterised by security requirements because they do not provide for the transfer of personal information over the network.

## **IX. ON THE CRITERIA OF ACCURACY AND EFFECTIVENESS**

### **A. Observations of institutional bodies, operators and associations**



**META** considers that the rules should take due account of the efforts and good faith shown in developing and implementing 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 can still misrepresent their age and access services and applications that were not designed for them. For this reason, it advocates a multi-pronged, multi-layered approach that combines different tools to facilitate age-appropriate experiences.

**AYLO**, while appreciating the Authority's willingness to collect metric data on the accuracy and effectiveness of age verification mechanisms and to set specific thresholds, considers that providing definitive recommendations on these issues goes beyond its remit and trusts the Authority's ability to assess and decide on these parameters, stressing the need for **measures that balance effectiveness with the principles of privacy and user data protection, also taking into account the risks we have highlighted with regard to any age verification or age estimation solution implemented at the website level**.

**ALTROCONSUMO** considers that the verification system should cover not so much the access device as the content accessed and sent. In fact, it believes that, to date, it is too easy to post a video on social networks that could violate any rule of privacy, decorum or even security. However, it argues that using a universal gatekeeper that only blocks access, according to an 'all or nothing' principle, does not solve the problem, and that rather we would need increasingly sophisticated (and stringent) control systems depending on the activity that is intended to be done online. It also points out that controlling a mobile phone is perhaps easier than controlling a PC (also because each mobile device corresponds to a registered user), whereas for PCs only the IP address can be traced, which can also be easily masked or falsified; In addition, there is a different access mode: on a PC, the browser is usually the gateway to all internet services, while on a mobile device apps are often used and this, in turn, requires two different approaches to the problem of how to control access, each with its own specificity.

**WEBGROUP** argues that, in general, in the case of platforms offering exclusively adult content, it would be **much more effective to achieve the AV at the device level through filtering software**. Moreover, from the point of view of effectiveness, it considers 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 the obligation of age verification. However, filtering software on devices can prevent minors from seeing all adult content, not only

those 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 takes note of the fact 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, so it refers to the documentation available in the literature and cited to in the measure.

# **X. ON THE CRITERIA OF ACCESSIBILITY, EASE OF USE AND NON-DISCRIMINATION**

## **A. Observations of institutional bodies, operators and associations**

**[OMISSIS - A video-sharing platform provider]** considers that it should be borne 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 the collection of personal data and user experience. The application of data-intensive methods not only increases the risk to data security, but can also discourage users from legitimate access to services. For example, the use of methods based on age assessment through the provision of an identity document can lead to a worsening of the user experience, as well as the sharing of unnecessary personal information, in particular when requested as part of a non-risk service such as, for example, a site to learn a new language online. Furthermore, when balancing the various rights, it is important to consider the plurality of users' needs and characteristics. Since not everyone has a credit card or identity document, verifying age using only rigid identifiers would risk excluding marginalised or socio-culturally disadvantaged groups from access to services and information, thus contributing to widening the cultural and economic gap. In addition, **[OMISSIS - A video-sharing platform provider]** considers that the age assurance mechanisms should include maximum commitment from industry to ensure that the solutions provided are simple and effective, including in the context of the exercise of supervision by parents and guardians. Only in this way will it be possible to promote users' trust in the process, while ensuring the effective protection of minors from adult content.

The **CNU** highlights the importance of user-friendliness and the accessibility criterion of the age assurance system, which must be respected by regulated entities in order to ensure that the age verification system is easily usable by all users, regardless of their characteristics and above all that it is accessible by users with disabilities, ensuring, for example, that there is the possibility of using screen readers 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 particular problems in terms of accessibility and that, in particular, minors reach a medium/high level of computerisation. Conversely, for the less computer-able groups, as for digital identity, there are more analogue channels such as activations at physical counters/shops that can also be used to certify age. Concerning the criterion of inclusivity and non-discrimination, it considers that in case the verification system leads to inaccurate or erroneous results, a review procedure could be envisaged at the request of the data subject or of the site/platform for a more accurate verification on the basis of certain data. For example, if the estimation system were to classify an older person as a minor, he or she could use the review procedure by presenting an identity document. Conversely, if the site/platform should 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 the collection of personal data and user experience. The application of data-intensive methods not only increases the risk to data security, but can also discourage users from legitimate access to services.

The Authority therefore favours the adoption of secure but, at the same time, user-friendly systems by citizens.

# **XI. ON THE TRANSPARENCY CRITERION**

## **A. Observations of institutional bodies, operators and associations**

**AYLO** fully supports the Authority's spirit of greater transparency, regardless of the verification or age estimation system used, and believes in the need to provide users,

both adults and minors, with clear and comprehensive explanations about any type of processing taking place on our platforms.

**WEBGROUP** reiterates that **age verification should be limited and performed in the personal device** and, on a subsidiary basis, the user should be informed to the extent required by data protection laws (GDPR), which would likely involve requiring the user's consent for the third party to become aware of the personal identity and age, solely for age verification purposes and to the exclusion of any other personal data, including knowledge of any internet activity of the user. To the extent required by law, the user should also be informed that the independent third party is certified by a certifying authority, whose role would be to organize the operation of age verification by the third party by providing the cryptographic specifications for the service and to certify the third parties (with the possibility of revoking the third parties if necessary).

**ALTROCONSUMO** considers that a vehicle for transparency is the use of infographics and tutorials by regulated entities, the Authority and certification bodies.

### **B. Assessments by the Authority**

The Authority agrees with the comments regarding the need for maximum transparency vis-à-vis users.

## **XII. ON TRAINING AND INFORMATION**

### **A. Observations of institutional bodies, operators and associations**

**AYLO** argues that the press, blogs and websites are useful tools to promote the importance of age verification and estimation and to raise awareness of the dangers and risks associated with the internet. AYLO declares that it has been dealing with age assurance mechanisms for many years and has conducted awareness-raising activities with the press and also through its sites regarding the dangers related to the verification and age estimation tools implemented at the website level. In addition, it states that the access page to their sites also includes a disclaimer and a request for a self-declaration of age aimed at dissuading underage users from visiting the sites. Furthermore, it considers that technical measures alone are almost never sufficient to solve social problems on their own and that adequate and effective protection of minors will never work meaningfully without parental participation. For this to happen, it is of the opinion that parents must first be able to participate meaningfully and that they should be trained as fully as possible on the typical behaviour of children and adolescents on the internet.

In particular, they should be informed about how their children use the internet and what its dangers and opportunities are. Finally, it welcomes any commitment by the Authority to improve the training of parents in this regard.

The **CNU** believes that only with a series of interventions, not only legal and regulatory, but also in the field of communication and digital education, will it be possible to make a concrete contribution so that there can be an effective age verification and therefore an increasingly effective protection of minors from the risks of the web.

The **COMMISSIONER FOR CHILDREN** considers that, in addition to technical solutions, extensive digital education and awareness-raising on the issue of protecting the physical and mental health of children online remains essential. This initiative must be carried out in advance and in parallel with the introduction of new technical tools that use all available information and training channels, activating all the appropriate institutional synergies and above all actively involving children themselves in the decision-making process regarding online protection policies, listening to their experiences, opinions and concerns to help develop more effective age assurance measures that respect their rights and wishes.

**ALTROCONSUMO** believes that consumer representative associations are a valuable channel of dissemination.

### **B. Assessments by the Authority**

The Authority certainly agrees with the respondents' comments regarding the need for adequate training and information for minors and parents themselves.