




The regulator of audiovisual  
and digital communication



Public consultation on the draft framework setting out the minimum technical requirements for age verification systems set up for access to certain online public communication services and video-sharing platforms that make pornographic content available to the public

April 2024



## Contents

<b>Contents.....</b>	<b>3</b>
<b>Introduction.....</b>	<b>5</b>
<b>The responsibility of targeted services broadcasting pornographic content</b>	<b>5</b>
<b>The evolution of the role of Arcom in the context of the bill to secure and regulate the digital space</b>	<b>6</b>
<b>The work already under way on age verification</b>	<b>7</b>
<b>Presentation of the framework.....</b>	<b>8</b>
<b>Supporting the sector in the implementation of age verification solutions</b>	<b>8</b>
<b>Updates of the framework and state of the art</b>	<b>8</b>
<b>Structure of the framework and implementation schedule</b>	<b>8</b>
<b>First part: reliability of age verification systems.....</b>	<b>10</b>
<b>Protection of minors by default</b>	<b>10</b>
• Criterion No. 1: tightness of age control.....	10
<b>Reliability criteria</b>	<b>10</b>
• Criterion No. 2: effectiveness of the solution.....	10
• Criterion No. 3: limiting the possibilities of circumvention.....	11
• Criterion No. 4: age verification at each service consultation.....	11
• Criterion No. 5: framework for the use of a user account.....	12
• Criterion No. 6: non-discrimination.....	12
<b>Second part: protection of privacy.....</b>	<b>13</b>
<b>Privacy protection principles</b>	<b>13</b>
<b>Implementation of a privacy-friendly age verification system by default and by design</b>	<b>13</b>
<b>Minimum requirements for all age verification systems</b>	<b>14</b>
• Criterion No. 7: independence of the age verification system provider in relation to targeted services broadcasting pornographic content.....	14
• Criterion No. 8: confidentiality vis-à-vis targeted services broadcasting pornographic content.....	14
• Criterion No. 9: confidentiality vis-à-vis proof of age generation providers....	14
• Criterion No. 10: confidentiality vis-à-vis any other third parties involved in the age verification process.....	15
• Criterion No. 11: safeguards for the rights and freedoms of individuals by age verifiers.....	15
<b>Specific requirements for privacy protection systems respecting the principle of ‘double anonymity’</b>	<b>15</b>
• Criterion No. 12: enhanced confidentiality vis-à-vis targeted services broadcasting pornographic content.....	16

---

• Criterion No. 13: enhanced confidentiality with regard to issuers of age attributes.....	16
• Criterion No. 14: enhanced confidentiality vis-à-vis any other third parties involved in the age verification process.....	16
• Criterion No. 15: availability and coverage of the population.....	16
<b>Informing users about the level of privacy attached to age verification systems</b>	<b>17</b>
• Criterion No. 16: explicit display of the level of user privacy protection.....	17
<b>Desirable objectives and best practices</b>	<b>17</b>
<b>Third part: alternative proof generation solutions accepted on a temporary basis.....</b>	<b>18</b>
<b>Fourth part: audit and evaluation of age verification solutions.....</b>	<b>19</b>
<b>Evaluation of the systems put in place under real conditions</b>	<b>19</b>
<b>Error rates, circumvention and risks of attack</b>	<b>19</b>
<b>Independence of the audit provider</b>	<b>19</b>

## Introduction

### The responsibility of targeted services broadcasting pornographic content

#### **1. With the democratisation of mobile devices allowing access to the internet for children, the exposure of minors to pornographic content on the Internet is rising rapidly.**

According to a study carried out by the Regulatory Authority for Audiovisual and Digital Communication (Arcom) on the basis of data provided by Médiamétrie, 2.3 million minors visit pornographic sites each month, with this number growing rapidly in recent years and linked to the democratisation of mobile devices among children. The proportion of minors visiting 'adult' sites has increased by 9 points in 5 years, from 19% at the end of 2017 to 28% at the end of 2022. Every month in 2022, more than half of boys aged 12 and over visited such sites, a figure that rises to two thirds for boys aged 16 and 17. On average, 12% of the audience for adult sites is made up of minors<sup>1</sup>.

Since the early 2000s<sup>2</sup>, research into the consequences of early exposure to pornography shows that exposing the youngest children to pornographic content can have **serious consequences** on their mental development and the image they form of sexuality and relationships between individuals, to the detriment of their personal development and greater equality in gender relations<sup>3</sup>.

#### **2. Since 1 March 1994, pursuant to the provisions of Article 227-24 of the Criminal Code, introduced by Law No 92-684 of 22 July 1992, it is prohibited to expose minors to pornographic content.**

The wording of this Article has been amended to clarify not only its scope, but also how it is to be assessed when an offence is recorded on the internet. In line with established case law, since 2020 Article 227-24 states that a mere declaration of age is not sufficient to prove age of majority<sup>4</sup>.. The wording currently in force is as follows:

*'The manufacture, transport, dissemination by any means whatsoever and irrespective of the medium of a message of a violent, inciting terrorism, pornographic nature, including pornographic images involving one or more animals, or likely to*

<sup>1</sup> Arcom, *Visits to 'adult' sites by minors* (based on data provided by Médiamétrie) published on 25 May 2023:

<https://www.arcom.fr/nos-ressources/etudes-et-donnees/mediatheque/frequentation-des-sites-adultes-par-les-mineurs>

<sup>2</sup> Mr. Arzano, C. Rozier, *Alice au pays du porno (Alice in Pornland): Ados : leurs nouveaux imaginaires sexuels (Teens: their new sexual imaginations)* Ramsay, 2005.

<sup>3</sup> See: <https://www.csa.fr/Informer/Toutes-les-actualites/Actualites/Quelles-solutions-pour-protger-votre-enfant-des-images-a-caractere-pornographique-sur-internet>; and B. Smaniotto (Researcher in Psychopathology and Clinical Psychology), 'Pornography: what impact on adolescent sexuality?', *The Conversation*, 28 August 2023: <https://theconversation.com/pornographie-quels-impacts-sur-la-sexualite-adolescente-207142>.

In this regard, Arcom also invites parents to consult the website:

<https://jeprotegemonenfant.gouv.fr/pornographie/>.

<sup>4</sup> Court of Cassation, Criminal Division, 23 February 2000, 99-83.928, <https://www.legifrance.gouv.fr/juri/id/JURITEXT00007070001>.

*seriously harm human dignity or incite minors to engage in games that physically endanger them, or to trade in such a message, shall be punishable by 3 years' imprisonment and a fine of EUR 75,000 when the message is likely to be seen or perceived by a minor.*

*Where the offences provided for in this Article are submitted by the print or audiovisual press or by online public communication, the special provisions of the laws governing these matters are to apply with regard to the determination of the persons responsible.*

*The offences provided for in this Article shall be constituted even if a minor's access to the messages referred to in the first paragraph results from a mere declaration by the minor that they are at least 18 years of age.'*

The legislator introduced, by Law No 2020-936 of 30 July 2020 to protect victims of domestic violence, **a special procedure involving Arcom with the aim of ensuring the full effectiveness of these provisions** on online public communication services making pornographic content available to the public on the internet.

This law thus entrusted the president of Arcom with a prerogative to issue formal notice to the publisher of a site to comply with the Criminal Code and, if this notice is not acted upon, to ask the ordinary judge to order Internet Access Providers (IAPs) to prevent access to this site.

**3. On the basis of these provisions, the Authority** issued 13 formal notices. It also referred the matter on 8 March 2022, **to the President of the Judicial Court of Paris to order the IAPs to block five of these services on formal notice**. This procedure is still ongoing on the date of publication of this public consultation.

### **The evolution of the role of Arcom in the context of the bill to secure and regulate the digital space**

The bill to secure and regulate the digital space (SREN), under discussion in Parliament, plans to update the system established by the Law of 30 July 2020.

Article 10 of Law No 2004-575 of 21 June 2004 on Confidence in the Digital Economy (LCEN), as drafted on the date of publication of this public consultation, provides that **Arcom 'establishes and publishes [...], after consulting the French Data Protection Authority, a framework for determining minimum technical requirements applicable to age verification systems**. These requirements concern the reliability of user age control and respect for their privacy. ' The scope of the system concerns 'pornographic content made available to the public by an online public communication service publisher, under its editorial responsibility, or provided by a video-sharing platform service within the meaning of Article 2 of Law No 86-1067 of 30 September 1986 on freedom to communicate' (hereinafter 'targeted services broadcasting pornographic content' or 'the targeted services'). Arcom may, where appropriate after obtaining the opinion of the President of the CNIL, give formal notice to one of these services to comply with this framework and, in the event of the infringement

persisting, after obtaining the opinion of the CNILTU, impose a financial penalty on it in accordance with the procedure laid down in Article 42-7 of the Law No 86-1067 of 30 September 1986. This public consultation concerns the draft framework provided for in these provisions.

The new powers conferred on Arcom by the bill would complement the powers otherwise granted to the judicial judge, who can be called upon directly to block a site that does not comply with the provisions of Article 227-24 of the Criminal Code.

## The work already under way on age verification

This document is part of the **work undertaken** in recent years by the CNIL on age verification solutions to reconcile the protection of minors and respect for privacy.

**The CNIL** first issued an opinion in June 2021 on the draft decree for the implementation of the 2020 law on implementing rules to protect minors from access to online public communication services broadcasting pornographic content<sup>5</sup>. To prevent people's sexual orientation – real or assumed – from being deduced from the content viewed and directly linked to their identity, the CNIL recommended from this notice to go through trusted third parties and made several recommendations,<sup>6</sup> which included a section on age verification. These publications were backed up by a communication published in July 2022 entitled '*Online age verification: striking a balance between protecting minors and respecting privacy*'<sup>7</sup> and the launch of a demonstrator of an age-verification mechanism that respects the privacy of users<sup>8</sup>, in cooperation with PEReN and a professor from the École Polytechnique.

The CNIL has already had the opportunity to recall that '*Contrary to what is sometimes said, the GDPR<sup>9</sup> is not incompatible with age control for access to pornographic sites, which is provided by law.*'<sup>10</sup>

Like the CNIL, Arcom also issued an opinion on the draft decree implementing Article 23 of the Law of 30 July 2020<sup>11</sup>.

It is in this context that **Arcom and CNIL, with the support of PEReN**, began joint technical exchanges with age verification actors in early 2023. These discussions were enriched by the feedback Arcom received from some of its foreign counterparts, who are also confronted with the challenges of protecting minors and privacy when controlling access to pornographic content.

<sup>5</sup> CNIL, Deliberation No 2021-069 of 3 June 2021 concerning an opinion on a draft decree on implementing rules on measures to protect minors from access to sites broadcasting pornographic content (see: <https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000044183781>).

<sup>6</sup> See: <https://www.cnil.fr/fr/la-cnil-publie-8-recommandations-pour-renforcer-la-protection-des-mineurs-en-ligne>

<sup>7</sup> See: <https://www.cnil.fr/fr/verification-de-lage-en-ligne-trouver-lequilibre-entre-protection-des-mineurs-et-respect-de-la-vie>

<sup>8</sup> See: <https://linc.cnil.fr/demonstrateur-du-mecanisme-de-verification-de-lage-respectueux-de-la-vie-privee>

<sup>9</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

<sup>10</sup> See CNIL press release of 21 February 2023: <https://www.cnil.fr/fr/controle-de-lage-pour-laces-aux-sites-pornographiques>

<sup>11</sup> CSA, Opinion No 2021-11 of 23 June 2021 on the draft decree on implementing rules on measures to protect minors from access to sites broadcasting pornographic content, <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000044174211>





## Presentation of the framework

### Supporting the sector in the implementation of age verification solutions

In accordance with the provisions of the bill, the draft framework shall specify the **technical requirements** expected both in terms of **reliability** in verifying the age of users (in this case their majority) and respect for their **privacy**.

The purpose of this framework is not to certify technical solutions. **The targeted services broadcasting pornographic content will remain free to choose their own solutions for the protection of minors, provided that they comply with the technical requirements of the framework.**

**The absence of an age verification system, as well as age verification systems with a degree of reliability or protection of privacy below the level of requirements established by this framework, will not be eligible.**

### Updates of the framework and state of the art

The framework **may be reviewed and updated** in order to take account of the state of the art. The SREN bill stipulates in this regard that the *'framework shall be updated as necessary under the same conditions'*.

It is indeed desirable that the sector adopt age verification solutions corresponding to the state of the art and to European and international standards, and compatible with industry practices, particularly with regard to existing technical protocols.

### Structure of the framework and implementation schedule

The first part of the draft framework concerns the reliability of age verification systems. In addition to the need to guarantee the protection of minors by default, i.e. even before accessing the service, it is necessary to specify the **conditions for the effectiveness of online age verification systems, while avoiding their circumvention.**

**All age verification systems must comply with all the requirements set out in this first part.**

The second part specifically deals with the protection of privacy by age verification systems deployed to control access to pornographic content. Sites may offer **age verification systems with different levels of privacy protection, subject to informing users of the level attached to each system.**

In this context, the draft framework establishes **minimum criteria for all age verification systems**, as well as reinforced specific objectives for the most privacy friendly systems known as 'double anonymity'. **Users will have to be offered at least one age verification system that complies with 'double anonymity' privacy protection standards.**

This second part also includes **best practices** in the field of data protection, considered desirable.

In addition, the targeted services broadcasting pornographic content will be able to implement, on a temporary basis, solutions for generating proof of age based on the **provision of a bank card, by way of derogation from the conditions laid down in the first and second parts, but subject to strict compliance with certain cumulative conditions set out** in the third part of this document.

Finally, the fourth and last part lays down the main principles likely to guide the services intended to broadcast pornographic content required to carry out an audit of their age verification systems. In particular, the **purpose** of such audits, the **conditions** under which they are carried out and the **requirements** applicable to third party auditors will be specified.

## **First part: reliability of age verification systems**

The purpose of this framework is to ensure the protection of minors by default, as soon as the first page of an online communication service enabling the broadcast of pornographic content is displayed.

### **Protection of minors by default**

The protection of minors entails **preventing** them from being **exposed** to pornographic content as soon as they access online public communication services making such content available.

In this respect, the SREN bill stipulates that targeted services broadcasting pornographic content are required to display a screen that does not contain any pornographic content **'until the age of the user has been verified'**.

- **Criterion No. 1: tightness of age control**

Targeted services broadcasting pornographic content must ensure **that no user accesses pornographic content until they have proven their majority**.

#### Examples and application

This protection of minors by default can be ensured, for example, by **completely blurring the service's homepage**.

Publishers can report the pornographic nature of their service. To do this, they can rely on a **self-declaration mechanism** [such as the RTA label<sup>12</sup>] set up on each page of their sites, enabling parental control systems to find out the minimum age required to access the content on the site, through response headers (or 'headers'<sup>13</sup>).

### **Reliability criteria**

To meet this standard, age verification systems (in this case majority) **must meet at least the following technical requirements**. These requirements are likely to evolve with the improvement of techniques and the placing on the market of new age verification systems.

- **Criterion No. 2: effectiveness of the solution**

---

<sup>12</sup> 'Restricted to adults'.

<sup>13</sup> The *headers* are information returned by the website server to the user's browser at the time of a request.

The technical age verification solution put in place by the targeted services broadcasting pornographic content **must make it possible to distinguish with certainty between minor users and adults.**

#### Examples and application

Where the technical solution put in place by the targeted services broadcasting pornographic content is based on an estimate of the user's age, it must be configured in such a way as to exclude the risk of a minor user being considered as being an adult ('false positives').

- **Criterion No. 3: limiting the possibilities of circumvention**

Targeted services broadcasting pornographic content must make their best efforts, in accordance with the industry's high standards of professional diligence, **to limit the possibilities of circumvention of the technical solutions they put in place.**

Age verification systems should not allow proof of age to be shared with other people.

Finally, the system must be robust in the face of the risks of attacks, such as *deepfakes, spoofing, etc.*

#### Examples and application

With regard to solutions based on an estimation of age by analysing facial features, the targeted services broadcasting pornographic content will have to ensure that the solutions include a **mechanism for recognising living persons**, the effectiveness of which is consistent with the state of the art. Detection shall be carried out by means of an image of sufficient quality and shall exclude any diversion process which may be used by minors in order to artificially appear to be adults, in particular by the use of photos, recorded videos or masks.

With regard to technical solutions for generating proof of age based on the presentation of a physical identity document, the targeted services broadcasting pornographic content must verify: (i) that the document is real, and that it is not a mere copy; (ii) that the user is the holder of the completed identity document. This verification may be carried out in particular by means of a facial feature recognition involving a life detection mechanism, under the conditions specified *above*.

- **Criterion No. 4: age verification at each service consultation**

Age verification must be carried out each time a service is consulted. The interruption of this consultation must trigger a new age verification if the user wishes to access pornographic content again.

Compliance with this criterion is without prejudice to the possibility for the user to use proof of age that can be reused or regenerated by himself, subject to the presence of a

second authentication factor. This can be done by linking the use of the reusable proof to the data subject's terminal, as is the case with digital *wallets*. Furthermore, the verification system must not allow this proof to be shared with another person or service.

### Examples and application

In the event of a consultation terminal shared between an adult and a minor, it is important to prevent the period of validity of the age verification from allowing pornographic content to be accessed without further verification. The validity of an age verification must therefore be interrupted when the user leaves the service, i.e. when the session ends, when the user quits the browser or when the operating system goes into standby mode and, in any case, after a period of [one hour] of inactivity.

- **Criterion No. 5: framework for the use of a user account**

The implementation of an age verification solution must not require the creation of a user account on the intended service providing pornographic content.

Furthermore, proof of age cannot be stored in a user account on such a service.

In any event, the age verification obligation applies to each access, with or without a user account.

- **Criterion No. 6: non-discrimination**

The solutions deployed by the targeted services broadcasting pornographic content must not have the effect of discriminating against certain population groups, in particular on the grounds set out in Article 21 of the Charter of Fundamental Rights of the European Union. Thus, the effectiveness of the technical age verification solution must be the same regardless of the physical characteristics of the user. In the case of proof-of-age generation systems based on *machine learning* or statistical models, service providers may, for example, test their solution on a variety of databases to ensure compliance with this requirement.

It is essential that age control systems **limit discriminatory biases, which also lead to errors that may call into question both their reliability and acceptability.**

Targeted services broadcasting pornographic content are invited to include any discriminatory biases, broken down on the basis of the relevant grounds of discrimination, when assessing the performance of their age verification system, but also in any audits they carry out (see *below*).

## **Second part: protection of privacy**

The purpose of this draft framework is also to ensure the **protection of privacy of the users** of age verification systems. These systems may pose high risks to personal data security, since age verification is similar to identity verification, and may therefore require the collection of sensitive data or identity documents.

Those involved in age verification systems must therefore pay particular attention to protecting the privacy of their users and the security of the information systems concerned, principles which the CNIL is responsible for ensuring are respected, in particular, the General Data Protection Regulation (GDPR).

### **Privacy protection principles**

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

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

- accuracy, proportionality and minimisation of the data collected;
- concise, transparent, understandable and easily accessible user information;
- appropriate data retention periods;
- possibility for individuals to exercise their rights, namely the right of access, the right to object, the right of rectification, the right to limit processing, the right to erasure, the right to portability;
- State-of-the-art security for information systems used to process personal data.

### **Implementation of a privacy-friendly age verification system by default and by design**

In 2022, the CNIL published a privacy-friendly age verification mechanism demonstrator for the transmission of an identity attribute (in this case proof of age)<sup>14</sup>.<sup>15</sup> In particular, the proposed mechanism will ensure that there is a watertight seal between the targeted services broadcasting pornographic content, which are obliged to check the age of their users, and third parties issuing age attributes.

This mechanism, known since then as 'double anonymity' or 'double confidentiality', has been developed and tested by various public and private actors, confirming its technical feasibility and its ability to meet the need for privacy protection inherent in online age verification mechanisms. It also corresponds to the objectives set in general for digital identity systems including attribute management. However, this mechanism,

<sup>14</sup> <https://linc.cnil.fr/demonstrateur-du-mecanisme-de-verification-de-lage-respectueux-de-la-vie-privee>

<sup>15</sup> <https://www.cnil.fr/fr/verification-de-lage-en-ligne-trouver-lequilibre-entre-protection-des-mineurs-et-respect-de-la-vie>

although referred to as 'double anonymity' in this document, is not 'anonymous' within the meaning of the GDPR, but nevertheless guarantees a high level of confidentiality.

**Online public communication services that make pornographic content available will have to offer their users at least one age-verification system that complies with 'double anonymity' privacy standards, ensuring that this system can be used by a large majority of its users.**

This requirement will enter into force at the end of the transitional period provided for in the third part of this framework, set at [...], without prejudice to the minimum requirements set out *below*. Thus, until that date, age verification systems will have to comply with the minimum set of requirements set out below in order to ensure an acceptable level of protection of the personal data of their users.

The following sections specify:

- the criteria applicable to all age verification systems covered by this framework;
- the specific objectives for the most privacy-friendly systems, known as 'double anonymity';
- the transparency obligations aimed at informing users of the level of privacy protection attached to the systems offered on the services;
- as well as good practices set out as desirable but not required to date.

### Minimum requirements for all age verification systems

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

- **Criterion No. 7: independence of the age verification system provider in relation to targeted services broadcasting pornographic content**

The provider of age verification systems shall be legally and technically independent of any online public communication service covered by this draft framework and ensure that targeted services broadcasting pornographic content have no access under any circumstances to the data used to verify the age of the user.

- **Criterion No. 8: confidentiality vis-à-vis targeted services broadcasting pornographic content**

The **personal data** enabling the user to verify his age with a communication service covered by this draft framework **must not be processed by this communication service**.

In particular, implementation of age verification solutions **shall not allow the communication services covered by this draft framework to collect the identity, age, date of birth or other personal information of such users**.

- **Criterion No. 9: confidentiality vis-à-vis proof of age generation providers**

Where the age verification system does not allow the user to obtain a reusable digital identity or proof of age, **the personal data provided by the user in order to obtain this attribute must not be retained by the proof of age generation provider.**

In addition, this type of system should not require the collection of official identity documents.

- **Criterion No. 10: confidentiality vis-à-vis any other third parties involved in the age verification process**

Where third parties other than proof-of-age generation providers are involved in the age verification process, e.g. for the management of proofs or billing of the service, **these third parties must not store any personal data of users of the system,** except for the storage of proof at the request of the user.

- **Criterion No. 11: safeguards for the rights and freedoms of individuals by age verifiers**

When determining whether or not a user can access an online public communication service on the basis of evidence submitted to it, the targeted service broadcasting pornographic content shall take an automated decision within the meaning of Article 22 of the GDPR. By refusing access to a service, that decision is likely to produce legal effects on the persons concerned, or at the very least, produce significant effects affecting people in a similar way.

The CNIL considers that such a decision may be based on the exception provided for in paragraph 2(b) of Article 22 of the GDPR, insofar as the targeted service broadcasting pornographic content is subject to an age verification obligation under Article 227-24 of the Criminal Code and, ultimately, the provisions of the P.J.L. SREN. Article 22.2.b of the GDPR requires that appropriate measures to safeguard the data subject's rights and freedoms and protective interests are provided for in the provisions authorising this automated decision.

In order to preserve privacy protection requirements aimed at limiting the ability of services to identify individuals, such measures must be put in place not by the targeted service broadcasting pornographic content, but by the provider of the technical age verification solution, whether it be the attribute provider or the issuer of proof. Such measures should enable users, in the event of an error, to challenge the result of the analysis of their attribute in order to obtain proof of age. For the exercise of these remedies, these age verification solution providers should offer users the option of using different attribute providers or, depending on the solutions, different issuers of proof.



The targeted service broadcasting pornographic content is nevertheless obliged to comply with the information obligations imposed by the GDPR and must inform users of the possibility of lodging a complaint with the provider of the age verification solution.

In any event, attribute providers must also allow individuals to rectify their data under Article 16 of the GDPR.

## Specific requirements for privacy protection systems respecting the principle of 'double anonymity'

**The following objectives complement the objectives of the minimum foundation to define a privacy-friendly standard for online age verification.**

- **Criterion No. 12: enhanced confidentiality vis-à-vis targeted services broadcasting pornographic content**

The requirements of Criterion No. 8 are supplemented by the following requirements.

An age verification system using 'double anonymity' should not allow the communication services covered by this draft framework 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 deduce the source or method of obtaining proof of age involved in a user's age verification process.

A 'double anonymity' age verification system must not allow these services to be able to recognise that two proofs of majority come from the same source of proof of age.

- **Criterion No. 13: enhanced confidentiality with regard to issuers of age attributes**

The requirements of Criterion No. 9 are supplemented so that an age verification system using 'double anonymity' must not allow proof-of-age generating providers to know for which service the age verification is carried out.

- **Criterion No. 14: enhanced confidentiality vis-à-vis any other third parties involved in the age verification process**

The requirements of Criterion No 10 are supplemented by the following requirements:

An age verification system using 'double anonymity' **should not allow any other third parties involved in the process to recognise a user who has already used the system.** For example, a third party providing proof of age or certifying its validity should not be able to know whether it has already processed proof from the same user.

- **Criterion No. 15: availability and coverage of the population**

The communication services covered by this framework must ensure that their users have **at least two different proof of age generation methods for obtaining proof of age through a 'double anonymity' age verification system.** In practice, a service provider offering a double anonymity solution must combine at least two methods of obtaining proof of age (e.g. a solution based on identity documents and one based on age estimation).

The communication services covered by this framework must ensure that a 'double anonymity' age verification system is available for at least **[80%]** of the adult population residing in France.

#### Examples and application

In practical terms, 'double anonymity' solutions must offer **several proofs of age generation providers** (e.g. different internet access providers and/or banks) and for other solutions, **different methods of age proof generation** (e.g. analysis of facial features and provision of identity documents).

### **Informing users about the level of privacy attached to age verification systems**

- **Criterion No. 16: explicit display of the level of user privacy protection**

**Each age verification solution must be explicitly associated with its level of privacy protection, so that solutions complying with the 'double anonymity' standards are displayed clearly and legibly.** In any case, other solutions should not be confused or promoted in order to mislead the user in favour of less privacy-protective solutions.

When a third party involved in the age verification process can be aware of the service for which the age verification is done, the user must be clearly informed.

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

## Desirable objectives and best practices

The following objectives are not yet required by age verification systems for compliance with this framework, but constitute **a set of best practices towards which age verification solutions should strive.**

### **Ability for users to generate proof of age themselves confidentially:**

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

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

- the system is based on *zero-knowledge proof*;
- the system is based on encryption techniques with the most complex attack resistance properties, even in the future.

## **Third part: alternative proof generation solutions accepted on a temporary basis**

**For a transitional period of [six months] from the publication of this framework**, designed to enable the services subject to them to identify and implement an age verification solution that meets all the criteria set out in first and second parts, solutions **using bank cards will be deemed to comply with the technical characteristics of the framework, subject to the following conditions.**

A solution using a bank card would be an initial method of filtering out some of the minors. This temporary solution is based on an infrastructure that has already been deployed and can be mobilised

Subject to compliance with the requirements below, this solution would initially enable to **protect the youngest minors**. Filtering can be carried out either in the form of a payment of EUR 0 or by simple authentication (without payment).

These verification systems:

- must not be implemented directly by the targeted services broadcasting pornographic content, but by **third parties independent of the service**;
- will have to **ensure the security of the verification** in order to prevent the risks of phishing associated with it. It is therefore important to ensure that payment information is entered on trusted sites. In this respect, it would be advisable for the targeted services broadcasting pornographic content and solution providers to launch a coordinated campaign to raise awareness of phishing risks, taking into account this new practice in particular;
- will have to enable at least **the existence and validity of the card** to be verified, which excludes a simple verification of the consistency of the card number;
- implement the strong authentication provided for in the European Directive (EU) 2015/2366 on payment services (known as 'PSD2'), for example by relying on the **3-D Secure Protocol** in its second version in force, to ensure that the service user is the cardholder by means of two-factor authentication.

**At the end of this transitional period, the conditions under which age verification by bank card could continue to be accepted will be clarified.**

## **Fourth part: audit and evaluation of age verification solutions**

The SREN bill stipulates that *'The Regulatory Authority for Audiovisual and Digital Communication may require publishers and service providers [...] to **conduct an audit of the age verification systems they implement in order to attest to the compliance of those systems with the technical requirements defined by the framework.** The framework shall specify the procedures for carrying out and publicising this audit, entrusted to an independent body with proven experience.'*

The following sections aim at clarifying the main principles likely to guide the targeted services broadcasting pornographic content that would be required to carry out such an audit.

### **Evaluation of the systems put in place under real conditions**

In order to ensure a high level of protection for minors, Arcom will evaluate the technical age verification solutions on a case-by-case basis, once implemented by the publishers, i.e. *in concreto*. Since certain solutions can be configured by the targeted services broadcasting pornographic content themselves, it is necessary to carry out an assessment under actual operating conditions.

Targeted services broadcasting pornographic content are required to ensure that the solutions put in place are systematically able to meet the requirements of the framework by adapting, where appropriate, their operating principles and parameters.

### **Error rates, circumvention and risks of attack**

The technical audit focuses on assessing, in general, whether the age verification solution complies with **all the criteria set out in this framework**.

In this respect, it particularly assesses:

- the ability of the technical solution to distinguish minor users;
- the absence of discriminatory bias;
- resistance to potential circumvention practices (*deepfakes* for example) and to the risks of attack<sup>16</sup>.

<sup>16</sup> The assessment of the risk of attack on an age verification solution is to determine whether the system is likely to be misused for fraudulent purposes.

## Independence of the audit provider

In order not to undermine the credibility of the audit, the auditor should have proven expertise and experience and be **independent** of both companies offering age verification solutions and the targeted services broadcasting pornographic content which use the said technical solution(s).

Arcom may, in a later version of this framework, specify the conditions under which audits must be carried out and made available to the public.

As things stand, and pending further clarification from Arcom, companies are encouraged to carry out technical audits of their age verification systems, initially within [...] months of publication of this framework and then at least **every year**.

Targeted services broadcasting pornographic content are also encouraged to **publish their audit report on an easily accessible page of their online interface, and in an easily understandable format** for the sake of transparency, especially with regard to users.