

cerre

Centre on Regulation in Europe



PROTECTION OF MINORS: AGE ASSURANCE

March 2025

Michèle Ledger



The logo for Cerre, consisting of the word "cerre" in a white, lowercase, sans-serif font centered within a solid blue square.

cerre

Issue Paper

Protection of Minors: Age Assurance

Michèle Ledger

March 2025



As provided for in CERRE's bylaws and procedural rules from its “Transparency & Independence Policy”, all CERRE research projects and reports are completed in accordance with the strictest academic independence.

The project, within the framework of which this report has been prepared, received the support and/or input of the following CERRE member organisations: Arcom, Amazon, BIPT, CnaM, EETT, Meta, Microsoft, Ofcom, Tencent. However, they bear no responsibility for the contents of this report. The views expressed in this CERRE report are attributable only to the authors in a personal capacity and not to any institution with which they are associated. In addition, they do not necessarily correspond either to those of CERRE, or of any sponsor or of members of CERRE.

© Copyright 2025, Centre on Regulation in Europe (CERRE)

info@cerre.eu – www.cerre.eu



Table of Contents

<u>ABOUT CERRE.....</u>	<u>3</u>
<u>ABOUT THE AUTHOR</u>	<u>4</u>
<u>1. INTRODUCTION</u>	<u>5</u>
<u>2. ECOSYSTEM OF NORMS AT THE EU LEVEL</u>	<u>8</u>
2.1 AGE ASSURANCE IS NOT MANDATED.....	8
2.2 THE DIGITAL SERVICES ACT AND THE AUDIOVISUAL MEDIA SERVICES DIRECTIVE	8
2.3 OTHER EU-LEVEL NORMS AND INITIATIVES	9
<u>3. ECOSYSTEM OF RULES IN EU MEMBER STATES</u>	<u>12</u>
3.1 FRANCE	12
3.2 IRELAND	13
3.3 ITALY	13
3.4 GERMANY	14
<u>4. INTERNAL MARKET ISSUES.....</u>	<u>16</u>
<u>5. AGE ASSURANCE IN THE UK AND IN AUSTRALIA</u>	<u>18</u>
5.1 UK	18
5.2 AUSTRALIA	19
<u>SUMMARY TABLE OF NATIONAL SYSTEMS</u>	<u>22</u>
<u>6. CRITICAL APPRAISAL OF THE EU FRAMEWORK</u>	<u>24</u>
<u>7. CONCLUSION</u>	<u>29</u>
FURTHER READING	30



About CERRE

Providing high quality studies and dissemination activities, the Centre on Regulation in Europe (CERRE) is a not-for-profit think tank. It promotes robust and consistent regulation in Europe's network and digital industry and service sectors as well as in those impacted by the digital and energy transitions. CERRE's members are regulatory authorities and companies operating in these sectors, as well as universities.

CERRE's added value is based on:

- its original, multidisciplinary and cross-sector approach covering a variety of markets, e.g., energy, mobility, sustainability, tech, media, telecom, etc.;
- the widely acknowledged academic credentials and policy experience of its research team and associated staff members;
- its scientific independence and impartiality; and,
- the direct relevance and timeliness of its contributions to the policy and regulatory development process impacting network industry players and the markets for their goods and services.

CERRE's activities include contributions to the development of norms, standards, and policy recommendations related to the regulation of service providers, to the specification of market rules and to improvements in the management of infrastructure in a changing political, economic, technological, and social environment. CERRE's work also aims to clarify the respective roles of market operators, governments, and regulatory authorities, as well as contribute to the enhancement of those organisations' expertise in addressing regulatory issues of relevance to their activities.



About the Author



Michèle Ledger is a researcher at the CRIDS research centre of the University of Namur where she also lectures on the regulatory aspects of online platforms at the postmaster degree course (DTIC). She has been working for more than 20 years at Cullen International and leads the company's Media regulatory intelligence service.



1. Introduction

According to a study conducted by the French regulator, ARCOM, 2.3 million minors visit pornographic websites every month. This number has been growing rapidly in recent years and is correlated with the democratisation of mobile terminals among children. The proportion of minors visiting ‘adult’ sites has risen 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 percentage that rises to two-thirds for boys aged 16 and 17. On average, 12% of the audience on adult sites is made up of minors¹.

Next to pornography content, there is also evidence that certain types of content pose a special risk for the development of children such as cyberbullying, sexual harassment, violence, and content that advocates dangerous or unhealthy or dangerous behaviours, such as self-harm, suicide and anorexia.²

In the European Union, according to a report from the European Audiovisual Observatory,³ access control measures are generally absent from some of the large Video-Sharing Platforms (VSPs) which tend to rely on self-declaration of users during the sign-up phase. The report also flags « an evident lack of initiative from most pornography providers to implement measures that prevent children from accessing their services and being exposed to their content ». It is true that the Audiovisual Media Services Directive that was revised in 2018 (and which introduced rules for VSPs) was finally transposed in all the Member States very late.⁴

Making sure that minors do not access harmful services and content that could impair their development has become in recent years a major concern for policy makers at the EU level, in some of the Member States and in other jurisdictions around the world.

The EU Digital Services Act⁵ (DSA) has introduced several rules on the protection of minors and the enforcement of these measures has become one of the enforcement priorities of the European Commission in relation to the Very Large Online Platforms it supervises. These rules also need to be enforced by the national competent authorities designated as such by the Digital Service Coordinators (DSCs).

Despite the fact that the DSA introduces fully harmonised rules on the protection of minors for the platforms in scope, some Member States are moving towards the adoption of rules to oblige websites

¹ Translated with DeepL.com (free version), source : <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000050385836>. The study was based on data supplied by Médiamétrie.

² The OECD also identifies that risks online for minors that are not only related to content, but more broadly to contract, conduct and contract (OECD 4Cs framework), available at <https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5df252f14&appId=PPGMS>

³ The protection of minors on VSPs: age verification and parental control, European Audiovisual Observatory, Strasbourg, 2023

⁴ 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.

⁵ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) OJ L 277, 27.10.2022, p. 1–102



to assess the age of users, either at the sign-up stage or when users wish to access content that is age restricted.

The Issue Paper:

- Explains **the ecosystem of EU provisions** that are directly or indirectly linked to **age assurance**;
- identifies some of **the Member States' initiatives on age assurance and their effects on the functioning of the internal market**;
- brings to light some recent initiatives from countries outside of the EU, namely Australia and the UK.

The paper does not examine the detail of the technical solutions for age assurance, nor does it take position on whether age assurance (age verification or age estimation) should be mandated.

Indeed, putting in place age assurance, and age verification in particular, carries important trade-offs, for **minors** (who may be deprived from accessing some content) **for adult users** (who will need to accept that a certain amount of personal data is collected) and for the **platforms** themselves (who will need to adapt and deploy the systems).⁶ These systems should not be deployed lightly, but should be clearly grounded and deployed in a proportionate manner.

The Issue Paper seeks to shed light on the current situation and to make recommendations on the areas where EU policy makers need to make decisions to arrive at a coherent set of rules at the EU level. Indeed, EU-wide harmonisation is desirable because the current fragmentation of national rules appears both detrimental to the protection of minors and to the deployment of pan-European digital services.

In this paper, we refer to **age assurance** as an umbrella term that covers methods used to determine an individual's age (or age range) with different levels of confidence or certainty.⁷ Self-declaration traditionally forms part of age assurance but it is widely recognised that this is not a reliable method since it can easily be circumvented. The report therefore focuses on:

Age verification which is “a system that generally relies on hard (physical) identifiers and/or verified sources of identification, to determine the individual's age or age-range, to a specified level of confidence, to provide a higher degree of certainty in determining the age or age-range of an individual than age estimation techniques”.

Age estimation which generally relies on estimation by reference to inherent features or behaviours related to the individual, to determine that the individual's age is likely to fall within an age-range, to a specified level of confidence, to provide a lower degree of certainty in determining the age or age-range of an individual than age verification techniques.⁸

⁶ Age Assurance, Guiding Principles and Best Practices, Digital Trust & Safety Partnership, September 2023, p.2

⁷ These definitions are in euCONSENT.. D5.1 Common Vocabulary. <https://euconsent.eu/project-deliverables/#>

⁸ Livingstone, S., Nair, A., Stoilova, M., van der Hof, S., & Caglar, C. (2024). Children's Rights and Online Age Assurance Systems: The Way Forward. *The International Journal of Children's Rights*, 32(3), 721-747. <https://doi.org/10.1163/15718182-32030001>



Protection of Minors: Age Assurance

These systems can be deployed to prevent minors from accessing certain services or certain content but also to provide children with appropriate experience depending on their (evolving) capacities.



2. Ecosystem of Norms at the EU level

2.1 Age assurance is Not Mandated

There are multiple norms at the EU level that point towards the need to prevent minors from accessing harmful content on the internet. However, none of these EU rules go as far as to define the type of content that should not be accessed by minors, they do not set a minimal age for accessing (certain types of) online services or content and they do not mandate age assurance. The EU wide norms have been put in place progressively over the years and the result is **an ecosystem of rules that are lacking clarity and coherence**. Some Member States are therefore filling the gaps, each in their own way, which is jeopardising the functioning of the internal market (see 3).

The EU level rules are listed in a Compendium of EU formal texts concerning children in the digital world, elaborated under the New Better Internet for Kids Strategy (BIK+).⁹ In relation to preventing minors from accessing certain content, the ecosystem of rules consists of two main legislative instruments: the Digital Services Act and the Audiovisual Media Services Directive, but other EU norms and initiatives also exist.

2.2 The Digital Services Act and the Audiovisual Media Services Directive

Historically, the first set of rules that obliged service providers to protect minors was contained in the Audiovisual Services Directive.¹⁰ The rules apply to linear and non-linear audiovisual services, over which providers have editorial control. Since 2018, rules also apply to Video Sharing Platforms.

According to Article 28b AVMSD, VSPs need to put in place “appropriate measures” to protect minors from content that could impair their physical, mental or moral development. **Age verification** is mentioned in the AVMSD as a possible way to ensure that minors do not have access to harmful content, but it is not mandated.

The DSA also contains rules that relate to the protection of minors and to age assurance/verification:

- Article 14 DSA obliges all intermediaries to specify any restrictions they impose in relation to the use of their service in respect of information provided by the recipients of the service, in their terms and conditions (T&C). They should also act in a diligent, objective and proportionate manner in applying and enforcing T&C with due regard to the rights and legitimate interests of all parties involved, including the fundamental rights of the recipients of the service. Where an intermediary service is primarily directed at minors or is predominantly used by them, the provider of that intermediary service shall explain the conditions for, and any restrictions on, the use of the service in a way that minors can understand. In short, all intermediaries should be transparent in restrictions of use in their

⁹ Available at <https://op.europa.eu/en/publication-detail/-/publication/8e18982d-0db6-11ef-a251-01aa75ed71a1/language-en>

¹⁰ Directive (EU) 2010/13 concerning the provision of audiovisual media services as amended by Directive 2018/1808



T&C and make sure to apply the rules they set for themselves.

- Article 28 DSA is one of the core rules as it specifies that online platforms (such as social media, video-sharing platforms, app stores and marketplaces) that are accessible to minors must take appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors. The Commission is set to issue guidelines on this article.
- Articles 34 and 35 whereby the online platforms (and search engines) designated by the Commission as very large (active monthly EU users above 45m) must annually assess negative effects of their services for the protection of minors, the rights of the child, and serious negative consequences for their physical and mental well-being, and mitigate any identified systemic risk. The list of possible mitigation measures they need to deploy includes age verification.

These norms have been analysed as implying a risk-based approach¹¹ which implies a tailored responses according in particular to the to the type of content available and the type of service.

2.3 Other EU-level Norms and Initiatives

GDPR

Article 8 of the General Data Protection Regulation (GDPR) provides that when data processing is based on consent and when online services are directly offered to children, the processing is lawful where the child is at least 16 years old. If the child is below 16 years, consent should be given or authorised by the holder of parental responsibility. However, the member states may set a lower age for when children can begin to give consent, as long as it is not below the age of 13.¹² This provision implies that online services that are offered to children should check the age of their users to make sure they are not under the age of consent for GDPR purposes. Also when age assurance is deployed, the rules of the GDPR will come into play regarding the data processing that is done by such mechanisms. This is not covered by this paper but has recently been addressed by the European Data Protection Board.¹³

The Rights of the Child

A key aspect of the discussion on age assurance is the need to take into consideration the rights of the child. Article 24 of the Charter of Fundamental Rights in the European Union enshrines the rights of the child and in particular, the right to be protected and the right to express views freely. The European declaration on Digital Rights and Principles for the Digital Decade contains a special title on the 'Protection and Empowerment of Children and Young People in the digital environment'. This non-binding but influential text highlights the need to (in relation to children and young people) promote positive experiences in an age-appropriate and safe digital environment; to provide opportunities to

¹¹ Livingstone et al (2024), p. 6

¹² Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

¹³ Statement 1/2025 on Age Assurance, 11 February 2025, available at https://www.edpb.europa.eu/system/files/2025-02/edpb_statement_20250211ageassurance_en.pdf



all to acquire the necessary skills and competences, including media literacy and critical thinking, in order to navigate and engage in the digital environment actively, safely and to make informed choices. Children and young people also need to be protected against harmful and illegal content, exploitation, manipulation and abuse online.

At the international level, the United Nations Convention on the rights of the child in relation to the digital environment states that “states parties should ensure that children have access to information in the digital environment and that the exercise of that right is restricted only when it is provided by law and is necessary for the purposes stipulated in Article 13 of the Convention” and that “any restrictions on children’s right to freedom of expression in the digital environment, such as filters, including safety measures, should be **lawful, necessary and proportionate**”. According to Article 13 restrictions are only allowed if they are provided by **law** and if they are necessary for the respect of the rights or reputations of others for the protection of national security or of public order, or of public health or morals.¹⁴

The European Digital Identity Framework (EUdi) Regulation

Article 5 (f) of the European Digital Identity Framework (EUdi) Regulation requires very large online platforms (VLOPs, but not very large online search engines) designated under the DSA to accept and facilitate the use of the European Digital Identity Wallet as a method for user authentication.¹⁵ In so doing, VLOPs need to respect the principle of data minimisation, meaning that they will only be able to require the necessary personal information for accessing the service. Further, according to the regulation, users are under no obligation to use the wallet to access the services and their access should not be hindered because they decide not to use the wallet.

Proposed CSAM regulation

A proposed regulation on the detection, reporting and removal of child sexual abuse material (CSAM) is in the course of adoption. While the proposal is aimed at providing a long term legal solution to enable the detection of CSAM in interpersonal communications services, it also targets hosting services (such as social media platforms and cloud services).

Providers would have to conduct regular risk assessments to assess the risk of dissemination of CSAM on their services and take mitigating measures. For instance, these risk assessments need to take into account functionalities enabling age-verification.

According to the Commission’s initial proposal, app stores would need to verify the age of users that want to access apps that carry a risk of grooming. The Parliament has proposed to only oblige app

¹⁴ Available at <https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child>. See also general comment N° 25 on the rights of the child in the digital environment, https://www.right-to-education.org/sites/right-to-education.org/files/resource-attachments/UN_CRC_General%20comment%20No.%2025%20%282021%29%20on%20children’s%20rights%20in%20relation%20to%20the%20digital%20environment_En.pdf

¹⁵ Regulation (EU) 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



stores designated as gatekeepers under the Digital Market Act to take certain measures to protect children in relation to apps that based on their information should not be accessed by children.

The Council had at the time of writing still not adopted its negotiating position on the text.

Better Internet for Kids Strategy (BIK+)

The Commission's Communication of 2022 on "a digital decade for children and youth: the new European strategy for a better internet" (BIK+) aims to ensure that children are protected and empowered in the new digital decade. In this document, the Commission announced that it will facilitate an EU code for age-appropriate design and requested a European standard on online age verification to be set up by 2024.¹⁶

Towards a Universal Age Verification Solution in the EU?

The European Commission published on 14 October 2024 a **call for tender to develop a « universal age verification solution »** to allow users to access an age-restricted online service by verifying their age, without requiring the sharing of added personal data. This solution could be used by social media platforms, gambling platforms or adult platforms. The call is specifically addressed to access the online services that are restricted to 18+, even if the solution should allow for age-appropriate access whatever the age restriction. The solution will be rolled out under the EUdi wallet.¹⁷ The Commission's overall aim with this procurement is to «seek a Europe-wide effective and convenient method to age-gate access to specific online services».

¹⁶ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:212:FIN>, see annual review for 2024 here: https://better-internet-for-kids.europa.eu/sites/default/files/2025-02/BIK_Report2024_WEB_0.pdf

¹⁷ https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/tender-details/docs/ae950883-112f-4139-989e-1c8d794bb77a-CN/EN_TENDER_SPECIFICATIONS_EC-CNECTLUX2024OP0073_Age%20verification%20solution_Part2_finalised_20241011_V1.pdf



3. Ecosystem of Rules in EU Member States

This section reviews national initiatives on age assurance in some of the Member States.¹⁸ Some of these initiatives derive from the transposition of Article 28b AVMSD on the protection of minors in relation to VSPs, while others target a wide range of services, and are potentially raising internal market concerns. The analysis of these national developments is useful on two accounts:

- First it shows why and how the member states are addressing age assurance
- Second it will shed light on the aspects that are challenged by the European Commission (see Section 4)

3.1 France

France adopted a law to secure and regulate the digital space ("Loi Sren") on 21 May 2024.¹⁹ The law requires the regulator (Arcom) to establish binding technical requirements ("référentiel") for age verification systems to be met by websites **that make available pornographic content** (Streaming/Video on demand services are also covered).

The standards were adopted on 8 October 2024. They require operators of porn services to refrain by default from displaying pornographic content until they have verified that the user is **at least 18** (either by blurring the home page or by using another mechanism such as the Restricted to Adults (RTA) label. Some of the other measures they need to take include:

- make available an age verification system that complies "with double anonymity" privacy protection standards;
- distinguish with certainty minors from adults and prevent circumvention (such as preventing the sharing of the proof of age with other people and avoiding the risks of attacks such as deepfakes, spoofing, etc.);
- avoid discrimination (e.g. the effectiveness of the age verification solution must be the same whatever the physical characteristics of the user);
- ensure that verification is carried out each time the service is consulted, without requiring the creation of a user account.

Arcom's référentiel also contains detailed requirements on the need to respect personal data standards.

The SREN law foresees that Arcom can request service providers to carry out audits of their age verification systems to assess them against the technical standards it established. These audits need to be carried out by independent organisations.

¹⁸ This account is partially based on Cullen International's Benchmark on Protection of minors : overview of initiatives on age-verification systems in European Countries, <https://www.cullen-international.com/client/site/documents/CTMEEU20240056> (updated November 2024)

¹⁹ <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000049563368>



The Law contains detailed rules on sanctions. In case of non-compliance with the formal notice to use age verification, Arcom can impose a financial penalty up to 3% of the provider's worldwide turnover, whichever is higher (and 5% of turnover in case of repeated non-compliance). Arcom is also empowered to request **Internet access service providers or domain name systems to block the URL addresses on non-compliant service providers. Search engines can also be ordered to delist services.** Fines are foreseen against intermediaries who do not prevent access.

Separately, France adopted a law to establish a digital age of majority and combat online hate on 7 July 2023.²⁰ It foresees that users must be at least 15 to register on social media platforms, unless their parents or holders of parental responsibility have given their consent. The law also specifies that social media platforms need to use technical verification systems as specified by Arcom's référentiel. The rules were set to apply to social media platforms that exercise their activity in France. The law has not been put into application, in view of its incompatibility with EU legislation (see below).

3.2 Ireland

The Online Safety Code of 21 October 2024 applies to **VSPs** and gives effect to Article 28b AVMSD.²¹ It aims in particular at protecting children from **pornography and extreme or gratuitous violence**. It requires VSPs that allow this type of content to use an "effective" method of "age assurance" to that "children" do not normally encounter this content. **Platforms will also need to use appropriate forms of age verification, depending on their size and nature, to protect children from video and associated content which may impair their physical, mental or moral development. For this purpose, this includes effective age assurance measures including age estimation.**

Children means a person under the **age of 18**. An effective age assurance cannot be based solely on self-declaration of age, but standards for effective age assurance are not specified in the code.

It is interesting to note that these rules only apply to the extent that the VSP's terms and conditions of use do not preclude the uploading/sharing of adult only video content. Next to the need to put in place effective age assurance, the VSPs also need to establish an easy-to-use content rating system to allow users to rate content as not suitable for children because the video content is adult-only and to tag the video content accordingly to ensure transparency for users that view the content.

Another interesting feature of the Irish system is that the systems that need to be deployed by VSPs to deal with complaints need to also address possible issues in relation to age assurance.

3.3 Italy

Law 159 of 13 November 2023²² requires **website operators and VSPs** (including streaming/VOD services) that disseminate **pornographic images and videos** in Italy to verify that users are **above the age of 18**.

²⁰ <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047799533>

²¹ As transposed in section 139K of the Online Safety and Media Regulation Act.

²² <https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2023-11-13;159!vig=2024-02-12>



The law tasks the regulator, AGCOM, with defining the procedural/technical measures. AGCOM announced the adoption of these measures on 7 October 2024. In a nutshell, website operators and providers of video-sharing platforms, that 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. The age assurance system must

- be certified and be legally and technically independent (from services that disseminate pornographic content). The services must in under no circumstance have access to the data used to verify the age of the user.
- carry-out the verification in two separate steps, i.e. identification and authentication (of the person identified), and for each usage session.

An age verification system using ‘double anonymity’, i.e. based on the intervention of an independent third party, should not allow the services 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.

For app-based systems (e.g. digital identity wallet app), the app certifies and generates the proof of age for the user, who can then provide the evidence to the visited website or platform. In other cases, the proof is issued by a specialised entity (or an entity that has identified the user in another context, but is in any case certified), and communicated to the user, who then presents it to the platform. The platform must then analyse the proof, and provide or deny access.

The authority clarifies that its approach is technology neutral and that platforms remain free to choose the system, provided that the systems comply with a set of principles.

3.4 Germany

According to Germany’s Interstate Treaty on the Protection of Minors²³, **pornographic content, certain listed content and content that is obviously harmful to minors** can only be distributed on the internet if the provider ensures that only **adults** have access to it by means of “closed user groups”²⁴.

Age verification systems are used as one way to control closed user groups. The rules apply to «telemedia providers» i.e. all electronic information and communications services, except telecoms services and to VSPs. Streaming/VOD providers are covered as well as operating systems and search engines.

The technical requirements for these systems are higher than the requirements for technical means that prevent access to content that is only likely to impair the development of minors. Accordingly, age verification to be used for closed user groups must involve two inter-related steps:

²³ <https://www.die-medienanstalten.de/service/rechtsgrundlagen/jugendmedienschutz-staatsvertrag/>

²⁴ Article 4(2) of the Treaty.



Protection of Minors: Age Assurance

- identification: proof of age must be carried out via personal identification (face-to-face contact)
- authentication: only identified and age-verified persons are granted access during the individual usage process.

To give certainty, the Commission for the Protection of Minors in the Media (KJM) can check and approve whether the “concepts” for the technical protection of minors meet the legal requirements. The KJM published criteria for the evaluation of these concepts.²⁵ It has approved 50 complete solutions and 48 partial systems (called modules)²⁶. The other key features of the German system is that this evaluation process is done at the request of service providers and the main responsibility for implementing the verification process lies with the content provider, which ultimately needs to make sure that pornographic content (and other content harmful to minors) is accessed only by adults.

²⁵ <https://www.kjm-online.de/themen/technischer-jugendmedienschutz/entwicklungsbeeintraechtigung/>. The KJM includes age evaluation for one-time use and for repeated use.

²⁶ <https://www.kjm-online.de/themen/technischer-jugendmedienschutz/uzulaessige-inhalte/>



4. Internal Market Issues

In the context of the regulatory transparency procedures set up under Directive 2015/1535,²⁷ Member States have notified to the European Commission their draft legislative initiatives on the protection of minors, including on age verification. Beyond the countries covered in this report, other countries, including Hungary and Spain have also notified draft laws covering these areas.

The European Commission has been issuing either detailed opinions or non-binding comments²⁸ to most of the notifying Member States, on the grounds that the draft national rules:

- are incompatible with the country of origin principle of the Electronic Commerce Directive²⁹ because they seek to impose obligations on ‘information society services’ offering their services in France, in addition to those imposed by the Member State where they are established; and/or
- undermine the full harmonisation approach of Article 28 DSA (a regulation does not normally require national implementation legislation; and/or
- overlap with the Commission’s monitoring and enforcement powers of the very large online platforms.

France received a detailed opinion from the Commission following the notification of its draft rules leading up to the adoption of the SREN Law.³⁰ France argued in its response that the age verification measures of the SREN law were proposed in the context of the transposition of Article 28b AVMSD, and that the rules apply to VSPs and to services over which the service providers have editorial control (hence services that are not in the scope of the DSA). The Commission in its reaction noted that the envisaged rules are not limited to VSPs but also cover other types of online platforms that are covered by the DSA. However, both the European Commission and the French authorities seem to agree that the French rules can be adopted so long as France revises its framework when sufficiently precise rules exist at the EU level for effective age verification. Also, it must be noted that the French rules on age verification and the removal of pornography apply to service providers based in France and outside the European Union. They also apply to providers established in another EU member state if the conditions to derogate from the country of origin principle are met. In this case, the measures apply three months after the publication of a joint ordinance by the ministers for culture and for digital technologies designating the service providers involved. Arcom can propose the designation to the ministers. France will probably notify another draft application decree of the SREN Law which foresees

²⁷ Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification) (Text with EEA relevance) OJ L 241, 17.9.2015, p. 1–15

²⁸ Detailed opinions have the effect of extending the standstill period (during which the Member State needs to refrain from adopting the final rules) by one additional month. During this period, the Member State needs to explain the follow up action it intends to take in response to the detailed

²⁹ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') OJ L 178, 17.7.2000, p. 1–16

³⁰ <https://technical-regulation-information-system.ec.europa.eu/en/notification/24221/message/105804/EN>



that VLOPs established in Cyprus (Pornbub, Stripchat) and the Czech Republic (XNXX, XVideo) will need to comply with Arcom's technical rules on age verification.

France did not receive a formal opinion following the notification of the law on the digital majority but the press reports that former EU Commissioner Thierry Breton sent a letter to the French minister for Europe and Foreign Affairs in which criticisms were voiced against the draft law.³¹

The Commission had no comments following the notification of the draft Online Safety Code, which online concerned VSPs established in Ireland.³²

Germany received a detailed opinion³³ on 1 July 2024 in which the Commission expressed serious concerns as to whether the draft Interstate Treaty on the Protection of Minors and Broadcasting is in line with the country of origin principle of the Electronic Commerce Directive or with the DSA.

Regarding the incompatibility with Article 3 of the Electronic Commerce Directive, the Commission notes that the provisions of the notified draft apply to information society services offering services in Germany and irrespective of their state of establishment and that despite the fact that the German authorities have stated their intention to enforce the notified draft on providers established outside of Germany on the basis of individual measures adopted by competent authorities, this is not reflected in the version notified by Germany.

Regarding the DSA, the Commission recalls that the Regulation establishes fully harmonised rules for a for a safe, predictable and reliable online environment. In particular, the Commission recalls that the protection of minors, a particularly vulnerable category of recipients of online intermediary services, is an essential aspect of the DSA. The Commission also recalls that, being a Regulation, the DSA does not allow for additional national requirements unless otherwise expressly provided. The Commission also notes that "the notified draft entrusts the supervision and enforcement of the notified draft, including the provisions falling within the fully harmonised field of the DSA, to the German media authorities (at various levels). This supervision and enforcement system under the notified draft would also apply with regard to service providers outside the jurisdiction of Germany and very large online platforms or very large online search engines in as much as they are covered by the scope of the notified draft. The Commission calls on the German authorities to ensure that the final law is aligned with the supervision and enforcement architecture of the DSA".

In short, the margin of manoeuvre of Member States wanting to impose age assurance obligation on platforms appears quite limited. The only option for Member States seems to be to impose such obligations on VSPs established in their member state. All other scenarios appear to be either in breach of the full harmonised approach of the DSA and - if the rules target information society service providers established in other Member States - of the Electronic Commerce Directive. The Commission also notes enforcement issues (see also the companion Issue Paper 'Charting the Path for Protection of Minors under the DSA').

³¹ https://www.linforme.com/tech-telecom/article/majorite-numerique-influenceurs-la-lettre-incendiaire-de-thierry-breton-au-gouvernement_1056.html

³² <https://www.cnam.ie/statement-on-the-online-safety-code/>

³³ <https://technical-regulation-information-system.ec.europa.eu/de/notification/25746/message/108751/EN>



5. Age Assurance in the UK and in Australia

5.1 UK

In the UK, following the adoption of the Online Safety Act³⁴, the regulator for the communications sector, Ofcom, is developing Children's Safety Codes with recommended measures that providers of services likely to be accessed by children need to take to comply with the Act.³⁵ Generally, Ofcom expects much greater age assurance, so that services know which of their users are children. All services which do not ban harmful content and those at higher risk of it being shared should implement "highly effective age assurance" (HEAA). Ofcom proposes that user to user (U2U) services use HEAA to restrict access to the whole service or from encountering certain types of identified content.

HEAA should be used to control access to an **entire service** if the service in question is deployed by a:

- U2U service whose principal purpose is the hosting or the dissemination of one or more kinds of PPC (Primary Priority Content: **pornographic content, suicide and self-harm content and eating disorder content**);
- U2U services whose principal purpose is the hosting or the dissemination of one or more kinds of PC (Priority Content: **abuse and hate content, bullying content, violent content, harmful substances content; dangerous stunts and challenges content**) AND who are high/medium risk for one or more of those kinds of PC.

HEAA should be used to prevent children from encountering **PPC identified** on a service:

- if the U2U service is not hosting or disseminating one or more kinds of PPC and which do not prohibit one or more kinds of PPC
- if the U2U service whose principal purpose is not the hosting or the dissemination of one or more kinds of PC; AND which do not prohibit one or more kinds of PC; AND are high/medium risk for one or more kinds of PC that they do not prohibit.

Interestingly, Ofcom considers that it is important to set consistent expectations for how service providers that allow pornographic content on their service implement HEAA to prevent children from encountering pornographic content, regardless of the type of service (U2U services or publishers of content).

All U2U services and search services need to carry out a **children's access assessment** to assess if the service (or part of it) is likely to be accessed by children. If the service is likely to be accessed by

³⁴ <https://www.legislation.gov.uk/ukpga/2023/50/enacted>

³⁵ <https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/284469-consultation-protecting-children-from-harms-online/associated-documents/vol5-what-should-services-do-to-mitigate-risks.pdf?v=336054#page=34?v=336054#page=34>



children, it will need to conduct a child risk assessment within a time that is also specified by Ofcom (3 months).

Ofcom does not recommend the use of specific age assurance methods but recommends that services take steps to fulfil criteria of technical accuracy³⁶, robustness³⁷, reliability³⁸ and fairness³⁹ (to ensure that their age assurance process is highly effective). Also, when implementing age assurance, the service providers need to make sure that age assurance is easy to use, including by children of different ages and with different needs. It is also desirable to ensure interoperability between different kinds of age assurance.

Ofcom has put forward a non-exhaustive list of kinds of age assurance that it considers possibly as highly effective⁴⁰, while also listing age assurance methods that are not highly effective⁴¹. Age assurance methods are developing rapidly and list of highly effective age assurance methods will expand over time. Like in other jurisdictions, Ofcom notes that age assurance methods involve the processing of personal data and hence, they should respect the requirements of the UK's data protection regime.

Ofcom has been assessing the age assurance measures on adult VSPs under the VSP regime that derived from the implementation of Article 28b AVMSD. This regime will be repealed once Ofcom's final codes on the protection of minors are adopted in April 2025.

On 16 January 2025, Ofcom published guidance for the industry on effective age checks to prevent children from encountering online porn and to protect them from other harmful content. Porn services have until July 2025 (at the latest) to introduce them and Ofcom will monitor compliance through an **enforcement programme**.⁴²

Interestingly also, the guidance specifies that services that publish their own pornographic content should put in place HEAA immediately, including certain Generative AI tools.

5.2 Australia

Australia enacted on 10 December 2024 the Online Safety Amendment (Social Media Minimum Age) Act 2024⁴³ which foresees that service providers must take reasonable steps to prevent children under 16 from being present on certain social media or from opening new accounts. Technically, the act

³⁶ This refers to the degree to which an age assurance method can correctly determine the age of a user under test lab conditions.

³⁷ This refers to the degree to which an age assurance method can correctly determine the age of a user in unexpected or real-world conditions.

³⁸ This refers to the degree to which the age output from an age assurance method is reproducible and derived from trustworthy evidence.

³⁹ This refers to the extent to which an age assurance method avoids or minimises bias and discriminatory outcomes.

⁴⁰ Open banking, photo-ID matching, facial age estimation, mobile network operator age checks, credit card checks, reusable digital ID services.

⁴¹ Self-declaration of age, age verification through online payment methods which do not require a user to be over 18; and general contractual restrictions.

⁴² <https://www.ofcom.org.uk/online-safety/protecting-children/age-checks-to-protect-children-online/>. The enforcement programme is available here : <https://www.ofcom.org.uk/online-safety/protecting-children/enforcement-programme-to-protect-children-from-encountering-pornographic-content-through-the-use-of-age-assurance/>

⁴³ <https://www.legislation.gov.au/C2024A00127/asmade/text>



modifies the Online Safety Act 2021, which established the eSafety Commissioner, while also setting up measures to combat cyberbullying towards children, cyber-abuse towards adults and the non-consensual sharing of intimate images.

The Online Safety Amendment (Social Media Minimum Age) Act 2024 will take effect within one year, on a date to be specified by the minister, with important details to be specified by the minister in charge and the eSafety Commissioner. Service providers that fail to comply with the age restrictions will face civil penalties. The minister in charge needs to specify (through legislative rules):

- The services in scope (the eSafety Commissioner will provide advice); and
- The type of information that cannot be collected (the eSafety Commissioner and the Information Commissioner will provide advice).

The eSafety Commissioner will formulate guidelines on age verification systems, following a consultation.

Australia's Online Safety Act requires that industry associations regulate certain types of online material through the development of codes of practices that need to be registered with the eSafety Commissioner, to become binding on all industry participants. If a code fails to meet the requirements of the law, the regulator can develop its own legally binding rules.

Phase 1 codes have been finalised⁴⁴ and are aimed at helping online service providers comply with class 1A and 1B material (i.e. the most seriously harmful online content, such as child sexual exploitation material and pro-terror material), while the **Phase 2 Code**, focussing on class 1C and class 2 material such as online pornography that is inappropriate for children, is in the course of development.

Australia's Phase 1 Code includes a special requirement for app distributors which is to 'make age and/or content ratings information about third-party apps available on the app distribution service to Australian end-users at the time those third-party apps are released on the app distribution service'.⁴⁵

The eSafety Commissioner issued a position paper on the development of phase 2 industry codes in July 2024⁴⁶) The regulator proposes that age rating systems are enforced on app distribution platforms, which could mean that they should take steps to confirm end-user's ages.

It is also noteworthy that in Australia, for these codes, a wide range of services are targeted, such as equipment services, search, and instant messaging services.

⁴⁴ https://www.esafety.gov.au/sites/default/files/2024-12/Phase-1-Codes-1A-and-1B-Regulatory-Guidance-Updated-Dec2024_2.pdf?v=1735996489216

⁴⁵ Measure 3 of the Phase 1 App Distribution Platform Distribution Code, <https://www.esafety.gov.au/industry/codes/register-online-industry-codes-standards>

⁴⁶ https://www.esafety.gov.au/sites/default/files/2024-07/Development-of-Phase-2-Industry-Codes-under-the-Online-Safety-Act-eSafety-position-paper_0.pdf?v=1735996489216



It must be noted that in Australia, content is **classified** according to the National Classification Scheme.⁴⁷ For instance class 2 material includes X18+ or R18+ content that may be harmful to children. This includes online pornography, high-impact depictions of violence or drug use, and from September 2024, computer games with simulated gambling, such as social casino games.

The eSafety Commission has already conducted some research in the context of the development of the Phase 1 and 2 Codes, including on age verification. It published an Age Verification Roadmap which examined approaches to address the risks and harms associated with children accessing online pornography.⁴⁸ Importantly, as any initiative on the matter in the EU, the Australian regulator sought to take “a human rights based approach, considering the rights, best interests and evolving capacities of children, as well as the rights of parents, carers, and other adults, including sex workers and performers and producers of online pornography... which aligns with the United Nations Committee on the Rights of the Child, supporting the child’s best interests while also respecting the rights of adults to consume and produce pornography in a safe and lawful manner”.

The regulator recommended that the government should undertake work on trial age assurance technologies before mandating their use. The aim of the trial is to support industry about how industry is expected to confirm the age of users.⁴⁹

This overview of these national developments shows that although the models examined have similar goals (except Australia, which is moving towards an outright ban of the use of social media for children under the age of 16), age assurance is addressed in different ways. There would be merit in having a more structured regulatory alignment across regions of the world, given the global reach of some of the players. For this, the EU should develop its own model and attempt to put an end to national fragmentation.

⁴⁷ <https://www.classification.gov.au/about-us/legislation>

⁴⁸ <https://www.esafety.gov.au/about-us/consultation-cooperation/age-verification#roadmap-and-background-report>

⁴⁹ The eSafety Commission published an issue paper on age assurance in July 2024, which is available at <https://www.esafety.gov.au/industry/tech-trends-and-challenges#age-assurance>



Summary Table of National Systems

	Type of content	Services in scope	Type of age assurance	Role of regulator	Other features
Australia	Certain social media	Certain social media	To be determined	<ul style="list-style-type: none"> To formulate guidelines To determine the services in scope 	
	-Seriously harmful online content - class 1C and class 2 material such as online pornography that is inappropriate for children	Also app distributors Search Equipment services Messaging services etc.	Regulator proposed that government should conduct a trial of age assurance	<ul style="list-style-type: none"> Register industry codes of conduct 	
France	Pornographic content	All websites that make content available	<ul style="list-style-type: none"> Double anonymity Prevent circumvention Avoid discrimination Respect personal data Ensure verification each time the service is accessed 	<ul style="list-style-type: none"> Sets technical requirements for age verification Can request service providers to carry out audits Enforcement and blocking orders 	Sanctions (up to 3% of worldwide annual turnover) Blocking orders can be ordered by regulator
Germany	Pornographic content and certain listed content that is obviously harmful to minors	All services except telcos	<ul style="list-style-type: none"> The overall aim of the systems are set by law (closed user groups) 	<ul style="list-style-type: none"> Regulator can check and approve systems 	Although the regulator may check that the system complies with the law, the responsibility for deploying the system lies with the service provider



Ireland	In particular, pornography and extreme gratuitous violence.	VSPs that do not preclude the upload of adult only video content	Not specified beyond that it needs to be an effective method of age assurance	Guidance	Complaints systems on VSPs need to deal with possible issues in relation to age assurance
Italy	Pornographic images and videos	Website operators, including and VSPs	Needs to be certified and technically independent from service provider Double anonymity	Sets procedural and technical measures	Operators that disseminate content must tell regulator who is in charge of age verification
UK	Pornographic content, suicide and self-harm and eating disorder content + abuse and hate content, bullying content, violent content, harmful substances content; dangerous stunts and challenges content	User to user services Publishers of pornography	Highly effective age assurance	<ul style="list-style-type: none"> ■ Regulator publishes non-exhaustive list of types of systems ■ Detailed enforcement programme 	Detailed enforcement programme



6. Critical Appraisal of the EU framework

This report shows that there is a significant amount of national fragmentation in the EU on age assurance. This could undermine the protection of minors since, depending on where the digital service provider is established, the level of protection will be different. This situation is not optimal either for pan-European service providers as they will incur significant compliance costs depending on the market.

Multiple factors explain this situation, some of which are linked to the EU-level rules themselves. This section reviews some of the issues and puts forward recommendations on possible solutions.

More clarity at the EU level on the type of services/content that should not be accessed by minors

A major difficulty with the EU level rules is that there is no EU-wide standard on the type of services or content that should not be accessed by minors. To date, there is no EU-wide definition of what constitutes harmful content leaving this to be determined at national level. Although it is extremely complex to define age-appropriate content across the Member States, which have culturally diverse communities, it may be possible to agree at the EU level that certain types of services or content are certainly harmful to children.

This approach is not entirely new at the EU level since in relation to TV, on-demand services and VSP, the AVMSD specifies that the most harmful content, such as gratuitous violence and pornography should be subject to the strictest measures.

The DSA refers to harmful content in a few instances but does not explain what harmful content covers, nor does it refer to particular types of harmful content for minors.

We see that at national level restricting access to pornography is a common concern, and that this takes place at the service level (e.g. Germany, France and Italy). Some of the legislations are also aimed at restricting access to other types of very harmful content.

The deployment of robust age assurance systems to prevent minors from accessing such content comes at a cost and there are trade-offs (such as additional personal data may need to be processed, the economic burdens of putting the systems in place, which could be difficult for new entrants or smaller companies, the fact that minors may be deprived from accessing etc).

These are not easy questions, but we see that on balance, something needs to be done, because the risk to minors seems high and because the risk of internal market fragmentation is also high.

We recommend that the guidelines seek to single out pornography (and possibly other types of very high-risk content such as gratuitous violence, suicide and self-harm). In relation to this content, the EU could recommend that effective age assurance technology **needs** to be used, provided the system complies with a set of principles such as the respect privacy and personal data in particular.



The guidelines should also seek to single out a **common age** to access such content. The age could be the age of majority (i.e. 18 in most Member States) or a younger age such as the age of consent (the age varies but according to Wikipedia, the oldest age in the EU is 17).

If the Member States continue to apply their own national systems or if the platforms do not comply, the EU may need to adopt a **targeted legislation** to specify these elements.

In relation to other (less serious forms of) harmful content, age verification is probably not desirable because of the high trade-offs would probably not outweigh the benefits of protecting minors from harm, also giving their fundamental right to access the online information. Other less intrusive forms of age assurance such as age estimation coupled with age-appropriate design would probably be sufficient.

The **content classification/age ratings** attached to different types of content are useful tools to help users to navigate through different types of content that could be harmful to minors, depending on their age groups. However, they are not easy to put in place in an environment where there is a lot of user generated content bearing in mind that the DSA includes a no general monitoring obligation.⁵⁰ In some industries (audiovisual and gaming in particular) there are effective voluntary age rating systems⁵¹ but this is not easy to replicate on platforms where the service provider does not have editorial control. In any event, the guidance could also seek to shed some light on these questions.

The articulation between the rules of the AVMSD and the DSA is not optimal and should be reassessed

VSPs are potentially covered by both sets of rules. A VSP is defined in Article 1 AVMSD as a service that has as its principal purpose (or as a dissociable section) or an essential functionality the provision of “programmes, user-generated videos, or both, to the general public, for which the video-sharing platform provider does not have editorial responsibility”... 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”. This definition overlaps with that of an online platform under the Article 3 DSA.⁵² This means that VSPs would potentially need to respect both sets of rules.

Although there may not be a direct incompatibility between the rules, since the AVMSD is a minimum harmonisation directive, the Member States are allowed to impose on VSPs established in their member states more detailed or stricter measures. This could therefore create a situation where age assurance could be mandated by a Member State for VSPs, whereas for other types of platforms, this would not be the case. This is in the spirit of the AVMSD, and the DSA itself recognises in recital 10 that the regulation should be “without prejudice” to other acts of Union law regulating the provision of information society services in general, regulating other aspects of the provision of intermediary

⁵⁰ Article 8 DSA

⁵¹ [PEGI](#) for the gaming industry and [Kijkijzer](#) for audiovisual content.

⁵² 'online platform' means 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.



services in the internal market or specifying and complementing the harmonised rules set out in this Regulation, such as the AVMSD (including its rules regarding VSPs). The DSA on the other hand, is aimed at fully harmonising the areas it covers, leaving no space for the Member States to introduce added rules.

Although the texts themselves recognise the coexistence of the rules, **in practice, the situation is not optimal:**

- **First**, it is legitimate to question the logic behind having a different legal treatment for VSPs compared to other types of online platforms. The scope of the AVMSD was broadened in 2018 to introduce rules to protect viewers and minors when they view audiovisual content on platforms, the logic being that audiences should be protected in a similar way than when the watch television and audiovisual media services on demand. Now that similar rules are introduced in the DSA for all types of online platforms, the rules of the AMVSD and how they have been transposed and put into application at the national needed to be assessed, to examine if they are still needed.
- **Second**, the **oversight of the rules will be different and may lead to complex situations**. In the case of the oversight and enforcement of the rules derived from the AVMSD, it is up to the regulatory authority of the country of establishment to assess whether measures chosen by VSPs are effective on a case-by-case basis. In practice the media regulator exercises this power and in case of breach of the rules, those derived from the transposition of the AVMSD will apply. In the case of enforcement of the rules derived from the DSA, the competent authorities designated under the DSA and the Digital Service Coordinator (DSC) are competent at the national level. For VLOPs and VLOSEs, the European Commission is the sole enforcer of Articles 34 and 35 on risk assessments and risk mitigation measures, whereas for the enforcement of the other rules, the competent authorities and the DSCs of the country of establishment are still potentially the enforcers (except if the Commission decides to take the lead).

This re-assessment should take place in the context of the upcoming review of the AVMSD which needs to take place by 19 December 2026 at the latest⁵³. The DSA foresees that by 17 November 2025, the Commission must report on the way the regulation interacts with other legal acts.⁵⁴

However, nothing precludes the European Commission from addressing these overlaps in the meantime.

Different rules for different types of intermediaries, content types and targeted users?

The tailored due diligence obligations introduced by the DSA are laudable and is a great step forward. Different obligations are introduced according to the type of intermediary, with more stringent

⁵³ Article 33 AVMSD.

⁵⁴ Article 91 DSA.



obligations to be complied with by respectively, mere conduit, caching, hosting, online platforms, and very large online platforms and search engines.

However, within these categories, the obligations do not differ, according to the type of content they convey, nor according to their expected category of users. Porn platforms are subject to the same obligations as any other type of online platform, even if the risk assessments and risk mitigation measures would need to be tailored to the specific risk incurred by minors. Likewise, article 28 DSA contains a proportionality criterion, but other than that the DSA does not treat such platforms - in a different manner.

Also, we note that under the DSA, only the VLOPS and VLOSES need to carry out **risk assessments**. However, this could be a useful tool for other platforms as well - especially **child specific risk assessments**. The European Commission could recommend in its upcoming guidelines that services that are available to users under the age of 18 could conduct risk assessment to examine whether (and if so, which) age assurance systems could be put in place.

Some online platforms argue that **app stores** (such as Apple App store and Google Play, which allow users to download applications on their devices) should be subject to added age assurance obligations. App stores assign age content ratings and require users to log in with their accounts. This means that they could in principle verify the age of users, which would have significant advantages as they often serve as gatekeepers for app downloads. Australia's Phase 1 Code includes a special requirement for app distributors which is to make age 'make age and/or content ratings information about third-party apps available on the app distribution service to Australian end-users at the time those third-party apps are released on the app distribution service'.⁵⁵ For Phase 2 Codes (regulating access to porn platforms for instance) the regulator proposes that age rating systems are enforced on app distribution platforms, which could mean that they should take steps to confirm end-user's ages.

This line of thought does not alleviate the need for the online platforms that are not app stores from ensuring a high level of privacy, security and safety of minors on their own services but since this added responsibility is also under consideration in Australia and the proposed CSAM regulation, the option of imposing added responsibilities on app stores merits more analysis.

Some services are out of scope of the EU legislative framework

As discussed in Section 2 some potentially high-risk services are not covered by the DSA (or by the AVMDs) such as online shops selling age restricted substances, adult content websites (with editorial responsibility), gambling websites and search engines (that are not very large or that only generate natural/generic links) . For these services, age verification obligations (if any) will only derive from national legislation, which will once more undermine the functioning of the internal market and hinder the deployment of pan-European services. Where it is proven that these gaps present risks for child protection, they should be filled to avoid an uneven level of protection of children.

⁵⁵ Measure 3 of the Phase 1 App Distribution Platform Distribution Code, <https://www.esafety.gov.au/industry/codes/register-online-industry-codes-standards>



What level of state intervention in age assurance systems?

The report shows various levels of regulatory intervention on the type of age assurance system to be used, even if no country imposes a given technology.

First, there are countries where the system is entirely left to the service providers, with a list of requirements to be fulfilled (Ireland) and/or a list of acceptable or non-acceptable systems (UK).

Second, there are countries where the level of intervention of the regulator is higher. France, Germany and Italy have a stronger oversight model as they are putting in place systems where the regulator needs to specify technical parameters, or where there is a need to conduct independent audits, or where there is the possibility to ask for clearance that the systems are in line with the legal requirements.

The EU should decide which of these models it would like to embrace.

EU policy decisions should be taken on the role to be given to the European Commission and to national competent authorities (if any). The sanctions in case of non-compliance (France provides that ISPs can be asked to block access to non-compliant services) could also be considered.

At the very minimum the European Commission could adopt a list of best practices for age assurance/verification tools. If it decides to oblige certain platforms to deploy age verification by adopting EU binding legislation, this legislation would probably also need to specify the role of the European Commission in setting the technical parameters, possibly by fostering EU standards⁵⁶.

A clear mention could in any event be made in the guidelines on consequences of using the European Commission's technical system developed under the universal age verification solution which is currently under development.

The rights of the child and other guiding principles

The rights of the child as envisaged in the EU Charter on Fundamental Rights (especially Article 24), the European Declaration on Digital Rights (in particular points 20-22), and the UN Convention on the Rights of the Child should remain the guiding principles when considering how to protect children from accessing services or content online.

A number of other core principles⁵⁷ on which age assurance solutions could be based could also be clearly articulated in the Commission's guidelines on Article 28 DSA and in any forthcoming legislation. The Commission could also specify if age verification solutions will also need to comply with the requirements of the EU Accessibility Act⁵⁸ and with the Cyber Resilience Act⁵⁹ once these enter in application.

⁵⁶ Such as the IEEE standard for Online Age Verification, <https://standards.ieee.org/ieee/2089.1/10700/>

⁵⁷ In particular, privacy preserving; proportionate to the risks and purpose, easy to use, secure; accessible; inclusive and interoperability.

⁵⁸ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L0882>

⁵⁹ https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202402847



7. Conclusion

This report highlights that the EU rules on age assurance are embryonic, whereas they are an important part of the ecosystem to ensure the protection minors of minors online. The Member States are therefore filling the gaps, which is creating internal market fragmentation, implementation difficulties for platforms that need to comply with the DSA and for competent authorities that need to enforce the rules.

The Commission's guidelines on Article 28 DSA are certainly needed but it is unclear, given their non-binding nature, if they will put an end to the appetite for national rules.

There are also some shortcomings in the EU legislation, since some services are not covered by the DSA (nor are they covered by the AVMSD). The articulation between the DSA and the AVMSD is not clear, which is could also lead to application difficulties. These difficulties will probably need to be resolved by legislation.

Turning to age assurance per se, and when looking at developments in other Member States (and regions of the world), we see that one of the most pressing issues is to decide if age verification should be mandated to prevent minors from accessing adult content services and possibly other high-risk content.

The EU should also clarify the level of state intervention for age assurance technology: none, mere guidance or a stronger oversight potentially with requirements to be specified, accreditation or auditing of technology. It also needs to decide on what are the respective roles of the European Commission and the national competent authorities.

Finally, the rights of the child and other guiding principles should be clearly articulated in the EU's normative system when adopting or recommending rules on age assurance.

This clarity would not only contribute to the protection of minors online but it would also allow pan-European services to be offered with more certainty across the EU. Ultimately, this would also enable the EU to develop its own 'regional approach' which could then be used to find some form of global alignment across different regions of the world.



Further Reading

European Commission: Directorate-General for Communications Networks, Content and Technology, New Better Internet for Kids Strategy (BIK+) – Compendium of EU formal texts concerning children in the digital world – 2024 edition, Publications Office of the European Union, 2024, <https://data.europa.eu/doi/10.2759/90437>




The protection of minors on VSPs: age verification and parental control, European Audiovisual Observatory, Strasbourg, 2023

Livingstone, S., Nair, A., Stoilova, M., van der Hof, S., & Caglar, C. (2024). Children's Rights and Online Age Assurance Systems: The Way Forward. *The International Journal of Children's Rights*, 32(3), 721-747. <https://doi.org/10.1163/15718182-32030001>

Research report : Mapping age assurance typologies and requirements, February 2024; Written by: Mohammed Raiz Shaffique LLM and Professor Simone van der Hof Center for Law and Digital Technologies (eLaw) Leiden University, Leiden, The Netherlands Part of the Better Internet for Kids (BIK) project coordinated by European Schoolnet (EUN) and commissioned by the European Commission.



Avenue Louise 475 (box 10)
1050 Brussels, Belgium
+32 2 230 83 60
info@cerre.eu
www.cerre.eu

-  Centre on Regulation in Europe (CERRE)
-  CERRE Think Tank
-  CERRE Think Tank

