Mapping age assurance typologies and requirements

Shaffique, M.R.; Hof, S. van der

Research report: Mapping age assurance typologies and requirements

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

February 2024

European Schoolnet
Transforming education in Europe
Better Internet for Kids
Universiteit Leiden
The Netherlands

EUROPEAN COMMISSION

Directorate-General for Communications Networks, Content and Technology
Directorate G — Data
Unit G.3 — Accessibility, Multilingualism and Safer Internet

E-mail: CNECT-G3@ec.europa.eu

European Commission
L-2417 Luxembourg

EUROPEAN COMMISSION

Research report: Mapping age assurance typologies and requirements

February 2024

Directorate-General for Communications Networks, Content and Technology
Better Internet for Kids (BIK)

Manuscript completed in February 2024

First edition

Luxembourg: Publications Office of the European Union, 2024

PDF ISBN 978-92-68-12845-9 doi: 10.2759/455338 KK-02-24-228-EN-N

Contents

Executive summary

The internet has afforded many novel opportunities to children, but also presents several potential or actual risks to their rights and well-being. On the one hand, children can participate in social interactions, create content, and voice their opinions online like never before but, on the other hand, they are increasingly exposed to different risks and harms online. Protecting children from online risks while furthering their participation in the online sphere is important, to ensure that the rights of children enshrined under the United Nations Convention on the Rights of the Child (UNCRC) and the Charter of Fundamental Rights of the European Union (CFREU) are upheld. In this respect, age assurance is considered one of the solutions towards creating a safe online experience for children while promoting their well-being and respecting their rights and best interests.

Age assurance is the umbrella term for the methods that are used to determine the age or age range of an individual to varying levels of confidence or certainty, and the three primary categories of age assurance methods are (1) age estimation, (2) age verification, and (3) self-declaration. While these are the directly relevant terms for the present report, associated concepts such as age-appropriate design and parental consent can also have an interrelation with age assurance.

The present report seeks to explore the various aspects of age assurance. At the outset, it is relevant to understand when and why age assurance must legally be used in certain cases and – in the absence of such a legal requirement – when (and in what form) it may be an adequate tool for the online protection of children.

Age assurance is legally relevant in three ways: (1) when a minimum age is prescribed by law for buying products or using services that may harm children or for performing legal acts, both of which require age assurance for legal compliance, (2) when there is a duty of care to protect children which may require age assurance to be employed, and (3) when there is a contractual obligation to provide the products or services only to users of a certain minimum or maximum age. Further, even where no legal or contractual stipulations exist, platforms may still undertake age assurance in certain circumstances out of their own volition.

Legal instruments at the EU level, such as the Audiovisual Media Services Directive (AVMSD), the General Data Protection Regulation (GDPR), the Unfair Commercial Practices Directive (UCPD) and Digital Services Act (DSA), and national laws on contract, sale of harmful products (e.g., alcohol, cigarettes, and weapons), provision of harmful services (e.g., gambling) etc., are relevant for consideration to ascertain the legal requirements for age assurance. It is crucial

to note that in situations where age assurance (or, in particular, age verification) is not legally mandated but can be employed as a duty of care to children or as a contractual obligation or a voluntary measure, it should still be implemented with due regard to the potential exclusionary effects of age assurance. This is because age verification can exclude children from (parts of) a service and thereby affect their participatory rights. Thus, other solutions such as age-appropriate design, age ratings, parental control tools etc., may be more appropriate in certain situations.

In scenarios where age assurance is to be implemented, an important factor that has to be determined is the type(s) of age assurance to be employed. In this regard, the present report discusses ten main methods of age assurance: (1) Self-declaration; (2) Hard identifiers; (3) Credit cards; (4) Self-sovereign identity; (5) Account holder confirmation; (6) Cross-platform authentication; (7) Facial age estimation; (8) Behavioural profiling; (9) Capacity-testing; and (10) Third-party age assurance services.

Each of these methods has varying assurance levels and associated advantages and disadvantages. For instance, self-declaration methods can be relatively privacy-friendly, but they provide a low level of assurance, as it is a trust-based method that can be easily circumvented. Facial age estimation can be easy to use but raises several privacy concerns as biometric data may be used for estimating age. The above methods are not an exhaustive list of age assurance methods present today and methods such as checking age against data held by entities including banks, mobile phone operators and credit reference agencies are also used in certain countries. Other methods, including estimation techniques using voice analysis, hand geometry, and natural language processing, could also become prominent in the future. Age assurance providers may also use a combination of age assurance methods instead of relying on any one method, which can potentially increase the level of assurance.

The liabilities associated with employing the right method of age assurance, in the appropriate manner, would depend on the applicable legal regime and the specific circumstances of the case within the context concerned. However, it can be construed that the primary responsibility for ensuring appropriate age assurance will be on the digital service providers themselves. Further, since the different types of age assurance have varying levels of certainty or accuracy, there have been initiatives to propose a mechanism to determine the confidence one can have regarding the accuracy of given age assurance methods. For instance, the International Organization for Standardization's (ISO) working draft on age assurance proposes a five-level model ranging from zero over basic, standard and enhanced, to strict, reflecting the level of confidence that can be placed on given age assurance methods implemented.

Given the above background, it is important to set out certain requirements that ought to be present, while assessing the necessity of age assurance and

determining the method of age assurance to be implemented. The present report discusses ten such requirements: (1) Proportionality; (2) Privacy; (3) Security; (4) Accuracy and effectiveness; (5) Functionality and ease of use; (6) Inclusivity and non-discrimination; (7) Furthering participation and access; (8) Transparency and accountability; (9) Notification, challenge, and redressal mechanisms; and (10) Hearing the views of children.

It must be acknowledged that there are significant challenges and tensions to be combated to achieve these requirements. Even among the requirements, there are contrasting principles and a balance needs to be struck between them. For instance, the accuracy of age assurance systems could contradict the privacy rights of users since increasing the accuracy of the age assurance employed could sometimes require users to provide more personal data to age assurance providers. This is, *inter alia*, why proportionality is a basic requirement that can play a role in satisfying the other requirements as extensively as possible.

Therefore, this report emphasises that age assurance is a complex matter, and it is far from straightforward as to how it is to be implemented in given situations. That is why age assurance should not be construed as a silver bullet for online child protection. Instead, it should be considered as one of the many tools to protect and further the experiences of children online. Going forward, the current efforts by European standardisation bodies could provide further clarity to age assurance providers on how to implement age assurance solutions in an appropriate manner. That includes the European standard for online age verification, as envisaged under the European Commission's Better Internet for Kids (BIK+) strategy, which will develop an interoperable approach to age verification across borders and sectors.

The previously outlined proposed standards could give more insight into aspects such as the levels of age assurance available for the protection of children that can be implemented by specific platforms. Furthermore, these standards should include consideration of the effects of age assurance on the digital ecosystem and, more specifically, on the effective enforcement of legislation, to ensure both adequate protection of, and age-appropriate design for, children, as well as the creation of a level playing field for companies. Additionally, any further guidance for online platforms, to provide them with assistance in applying measures that can ensure a high level of privacy, safety and security for children, while respecting their fundamental freedoms, would be welcome. The European Commission is empowered to issue such guidelines under Article 28 (4) DSA, which could include guidance on the application of age assurance methods.

1. Introduction

The internet has drastically changed our lives in the past few decades, and with that, has also provided a range of new opportunities for everyone, which have empowered, in particular, children and young people. For instance, children have utilised the tools provided by social media platforms to mobilise and to voice their opinions on social issues.[1] However, these new affordances do come with corresponding drawbacks, such as the various risks children face on the internet, including online content, conduct, contact and consumer risks.[2] For instance, children are exposed to cyberbullying that is "*far more severe in scope and the potential harm it can create*" as compared to traditional forms of bullying.[3] Thus, it has become ever more important to protect children from such risks without depriving them of any of the rights afforded to them and the benefits the internet could provide.

The rights of children are enshrined in the United Nations (UN) Convention on the Rights of the Child 1989 (including its optional protocols) (UNCRC)[4] and Article 24 of the Charter of Fundamental Rights of the European Union (CFREU).[5] Whenever this report refers to the rights of children, we mean the rights of children under these legal frameworks. Against this background, policymakers, civil society groups and other organisations have considered age assurance as one of the solutions for the protection of children online. The European Commission's Better Internet for Kids (BIK+) strategy, which was published on 11 May 2022,[6] safeguards the protection of children against online risks, promoting children's well-being by creating safe and age-appropriate digital environments and respecting children's rights and their best interests in

[1] Tisdall, E. K. M., & Cuevas-Parra, P. (2022). Beyond the familiar challenges for children and young people's participation rights: The potential of activism. *The International Journal of Human Rights*, *26*(5), 792-810.

[2] OECD. (2021). *Children in the digital environment: Revised typology of risks*. https://www.oecd-ilibrary.org/science-and-technology/children-in-the-digital-environment_9b8f222e-en; Livingstone, S., & Stoilova, M. (2021). The 4Cs: Classifying online risk to children. *Leibniz-Institut Für Medienforschung | Hans-Bredow-Institut (HBI)*. https://doi.org/10.21241/ssoar.71817.

[3] van Tiel, J. (2020). *Cyberbullying, an overlooked and ever growing danger to the development of children*. Technical report, KidsRights.

[4] As elaborated by the Committee on the Rights of the Child with respect to the digital environment, in: Committee on the Rights of the Child. (02.03.2021). *General comment No. 25 (2021) on children's rights in relation to the digital environment*. CRC/C/GC/25. https://digitallibrary.un.org/record/3906061?ln=en.

[5] *OJ C 326, 26.10.2012, p. 391–407.*

[6] European Commission. (11.05.2022). *A Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+)*. https://digital-strategy.ec.europa.eu/en/library/digital-decade-children-and-youth-new-european-strategy-better-internet-kids-bik.

general. One of the objectives of the BIK+ strategy is to formulate a European standard for online age verification.[7]

Thus, the present report seeks to explore the various dimensions of age assurance, providing a first robust evidence base drawing together relevant typologies and requirements at play in the current digital ecosystem.[8] This report will meet a two-fold purpose, which is (1) to provide a better understanding of the existing and still-developing types of age assurance that can be distinguished in the market and (2) to identify the requirements to be taken into consideration to ensure balanced and context-based approaches to age assurance. To further the understanding of age assurance, and particularly its role in the online protection of children, it is also relevant to first explain when and why age assurance must legally be used in certain cases and – in the absence of such a legal requirement – when (and in what form) it may be an adequate tool for the online protection of children.

In terms of the structuring of this report, first, we provide a better understanding of the relevant terms for this study (section 2). Second, we explain how age assurance and, more specifically, age verification are relevant from a legal perspective (section 3). Third, the forms (typologies) of age assurance are identified and explained (section 4). Finally, this report identifies the requirements for age assurance for those cases where it is a mandatory or adequate tool for protecting children online (section 5). The report ends with a conclusion (section 6).

[7] European Commission. (11.05.2022). *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. A Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+)*. COM(2022) 212 final. Pg. 11. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022DC0212. Though we focus primarily on European Union (EU) law, it is worth mentioning that age assurance also features as a possible solution in the Online Safety Act 2023 recently passed by the United Kingdom's Parliament, https://www.legislation.gov.uk/ukpga/2023/50/contents/enacted.

[8] The current research project on age assurance builds on the research conducted under the euCONSENT project, among others in deliverable D2.3 - 'Methods for Obtaining Parental Consent and Maintaining Children Rights'. This project adds to the studies carried out in euCONSENT by going into more detail on the legal analysis of age assurance, providing a classification of types of age assurance, including their advantages and disadvantages, as well as a further elaboration of the requirements for age assurance. For euCONSENT, see https://euconsent.eu/.

2. Relevant terminology

In this section, we discuss the relevant terminology for this study. First, there are concepts directly related to age assurance, and then there are terms that are often mentioned in connection with age assurance (i.e., associated terms).

2.1. Directly related terms

Age assurance is the umbrella term for the methods that are used to determine the age or age range of an individual to varying levels of confidence or certainty.[9] The three primary categories of age assurance methods are **age estimation**, **age verification** and **self-declaration**.[10]

Age estimation consists of methods which establish that *"a user is likely to be of a certain age, fall within an age range, or is over or under a certain age. Age estimation methods include [estimation based on facial features,][11] automated analysis of behavioural and environmental data, comparing the way a user interacts with a device with other users of the same age, and metrics derived from motion analysis or by testing their capacity or knowledge".*[12]

Age verification is *"a system that relies on hard (physical) identifiers and/or verified sources of identification that provide a high degree of certainty in determining the age of a user. It can establish the identity of a user but can also be used to establish [whether the user is over a certain minimum or under a certain maximum][13] age only*".[14]

Self-declaration is a category of age assurance which consists of methods that rely on the individual to supply their age or confirm their age range, without providing any evidence to prove such declaration.[15] Examples of self-declaration methods include declaring one's date of birth or declaring that one is above 18 years of age.

---

[9] euCONSENT. (29.06.2021). *D5.1 Common Vocabulary*. Pg. 4. https://euCONSENT.eu/project-deliverables/.

[10] *Id*.

[11] Added by the authors.

[12] CEN and CENELEC. (Sep 2023). *Age appropriate digital services framework*. Pg. 10. https://www.cencenelec.eu/media/CEN-CENELEC/CWAs/ICT/cwa18016_2023.pdf.

[13] Added by the authors.

[14] CEN, *supra* note 12 at 10.

[15] ICO. (14.10.2021). *Information Commissioner's opinion: Age Assurance for the Children's Code*. Pg. 14. https://ico.org.uk/media/about-the-ico/documents/4018659/age-assurance-opinion-202110.pdf.

Age assurance providers, as mentioned in this report, include digital service providers and platforms (used interchangeably) who provide their services online and perform their own age assurance. It also includes third parties who provide age assurance solutions.

There are two useful takeaways regarding the above terms. First, when it comes to ascertaining the age of an individual, certain literature uses the term age verification as the broader umbrella term instead of age assurance.[16] However, for the purpose of the present report, age assurance is used as the umbrella term and age verification is used as a category of age assurance, in line with the position adopted by the euCONSENT,[17] the European Committee for Standardization (CEN) and the European Committee for Electrotechnical Standardization (CENELEC).[18] Second, it is clear from the definitions of age estimation and age verification that there is a gradual yet important difference between these terms. Whereas in age estimation, you try to get as accurate a picture as possible of someone's age, or at least the age range within which the person is situated, age verification aims to establish what someone's age is, or at least whether a person is above a certain minimum age, or is below a certain maximum age (so-called verification[19]), without necessarily knowing what their actual age is.

2.2. Associated terms

Some concepts are not directly about determining the (minimum or maximum) age of users, including children, of digital services but may be associated with age assurance and, hence, relevant.

Age-appropriate design covers the design of digital services (including terms and conditions and policies) *"that are (1) suitable for children in general taking into account their rights and well-being, including rights specific to children such as the right to play, and (2) suitable for children given their specific age or stage*

[16] See DPC. (Dec 2021). *Fundamentals for a Child-Oriented Approach to Data Processing*. Pg. 44. https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf; European Parliamentary Research Service. (Feb 2023). *Online age verification methods for children*. https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/739350/EPRS_ATA(2023)739350_EN.pdf.

[17] euCONSENT, *supra* note 9.

[18] CEN, *supra* note 12.

[19] "[*T]he process of verifying specific identity attributes or determining the authenticity of credentials in order to facilitate authorization for a particular service",* see World Bank. (2019). *Identification for Development (ID4D), Practitioner's Guide*. Pg. 222. https://id4d.worldbank.org/guide.

of development, pursuant to the evolving capacities of children as referred to in Article 5 UNCRC".[20]

Age gating refers to the phenomenon where technical measures are "*used to restrict or block access for users that do not meet an age requirement*".[21]

Age ratings are systems used to label the minimum age recommendation for using products or services such as games, films, mobile apps, etc., which can guide stakeholders by reflecting the suitability or harmfulness of a product or service for a child.[22]

Age token is a digital token issued by an age assurance provider that only contains information pertaining to the specific age or age range or confirmation (or rejection) of the sufficiency of the age of a user.[23]

Parental consent means the grant of consent from a person who has parental authority over a child who is under 13 to 16 years old (depending on national law), for the processing of the child's personal data, [24] as envisaged under Article 8 of the General Data Protection Regulation (GDPR)[25]. Note that other laws may require parental permission for children to engage in, e.g., performing a legal act, such as the conclusion of a contract.

Parental control includes tools that can be used by parents to protect children, e.g., from inappropriate content online, through filtering content and monitoring online activity.[26]

As can be seen, age assurance has an interrelation with concepts such as age-appropriate design and parental consent in as much as age assurance may be helpful in implementing age-appropriate design or required to ascertain whether parental consent is needed. However, the scope of age assurance is much wider and is not restricted to these concepts.

---

[20] CEN, *supra* note 12 at 9.

[21] 5Rights Foundation. (Oct 2021). *But how do they know it is a child? Age Assurance in the Digital World*. Pg. 6. https://5rightsfoundation.com/uploads/But_How_Do_They_Know_It_is_a_Child.pdf.

[22] Pan European Game Information. (n.d.). *PEGI age ratings*. https://pegi.info/page/pegi-age-ratings.

[23] 5Rights Foundation, *supra* note 21 at 38-39.

[24] van der Hof, S., & Ouburg, S. (2021). Methods for Obtaining Parental Consent and Maintaining Children Rights, WP2: Existing Methods, User Needs and Requirements. Deliverable D2.3 euCONSENT. *Leiden University*. Pg. 12.

[25] 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, *OJ L 119, 4.5.2016, p. 1–88.*

[26] euCONSENT, *supra* note 9 at 15.

3. Legal analysis of age assurance

This section explains when and why age assurance must be used legally and – in the absence of such a legal requirement – when it may be considered as an adequate tool for the online protection of children and their rights and well-being. In doing so, it is first important to point out that age assurance is legally relevant in three ways:

(1) when a minimum age is prescribed by law for buying products or using services that may harm children or for performing legal acts, both of which require age assurance for legal compliance,

(2) when there is a duty of care to protect children, which may require age assurance to be employed, and

(3) when there is a contractual obligation to provide the products or services only to users of a certain minimum or maximum age.

Laws are required to protect children and their rights in the online sphere *inter alia* because of the myriad of risks faced by children online that may result in harm to children's rights, well-being and development. The Organisation for Economic Co-operation and Development (OECD) has published a risk model which highlights the main risks faced by children in the digital environment, i.e., content risks, conduct risks, contact risks, consumer risks and cross-cutting risks (i.e., advanced technology risks, health risks and privacy risks).[27]

As regards the harms that can be suffered by children online, it bears mention that harm is a comprehensive concept and covers various types of harms to the development and well-being of children, such as harms to the child's physical, mental, spiritual, moral, psychological and social development.[28] The harm faced could include economic damage (e.g., gambling, contracts, and the profiling of children), physical or mental health damage (e.g., the use of alcohol or drugs, gambling and the profiling of children), and damage to social or moral

[27] OECD, *supra* note 2; see also Livingstone, *supra* note 2.

[28] Livingstone, S. (2013). Online risk, harm and vulnerability: Reflections on the evidence base for child Internet safety policy. *ZER: Journal of Communication Studies*, *18*(35), 13-28. Pg. 21. https://www.researchgate.net/publication/285900088_Online_risk_harm_and_vulnerability_Reflections_on_the_evidence_base_for_child_internet_safety_policy; see also Committee on the Rights of the Child. (Nov 2003). *General Comment No. 5 (2003) General Measures of Implementation of the Convention on the Rights of the Child (Arts. 4, 42 and 44, Para. 6)*. CRC/GC/2003/527. https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsiQqI8gX5Zxh0cQqSRzx6Zd2%2FQRsDnCTcaruSeZhPr2vUevjbn6t6GSi1fheVp%2Bj5HTLU2Ub%2FPZZtQWn0jExFVnWuhiBbqgAj0dWBoFGbK0c.

development (e.g., gambling, the use of weapons and the profiling of children).[29]

With respect to the relation between harm and risk, it has been stated that "*risk is a harm that is yet to happen*" and "*harm is a risk that has been realised*".[30] Because it may be difficult to predict or assess the (long-term) online harms to children's physical, mental, spiritual, moral, psychological and social development (Article 6 UNCRC), and their rights more generally, and because the likelihood and impact of online harm may be greater for children, a precautionary approach is called for.[31] Such an approach is intrinsically linked to the best interest of the child (Article 3 UNCRC)[32] and entails legally prohibiting or otherwise restricting certain practices when they raise serious concerns in relation to the risk of harm to children.[33] Both when practices are legally prohibited or should be restricted for children, age assurance may be relevant. Moreover, as we explain further when identifying and analysing requirements for age assurance (see section 5), this approach is relevant when determining whether the implementation (of a specific type) of age assurance is proportional to the risk involved.

Given the above background, it is pertinent to further analyse the three ways in which age assurance is or could be required by law.

3.1. Legally mandated age verification

The law sets requirements for performing a legal act or for a minimum age when products or (certain practices within) digital services may cause harm to children. Within both these categories, age verification is a necessary measure because the law explicitly states so, or the law can only be complied with if it is known whether a user has reached the minimum age set by the law.

First, examples of laws that have minimum ages set for the performance of legal acts are contract law and data protection law. The legal capacity to

[29] Data protection can include harm resulting from data-driven services that, for example, spread disinformation and unhealthy content or profiling children for commercial purposes, such as targeted advertising or monetised matchmaking.

[30] 5Rights Foundation. (Oct 2020). *Building the Digital World that Young People Deserve. Priorities for the Online Harms Bill*. Pg. 20. https://5rightsfoundation.com/uploads/5rights-priorities---online-harms-bill.pdf.

[31] Lievens, E. (2021). Growing up with digital technologies: how the precautionary principle might contribute to addressing potential serious harm to children's rights. *Nordic Journal of Human Rights*, *39*(2), 128-145; see also Committee on the Rights of the Child, *supra* note 4.

[32] Eekelaar, J. & and Tobin, J. (2019). Art. 3 the Best Interests of the Child. In Tobin, J. (Ed.), *The UN Convention on the Rights of the Child: A Commentary* (p. 99). Oxford: Oxford University Press.

[33] Lievens, *supra* note 31.

conclude a contract is regulated by national law, however, generally speaking, the minimum age for legal capacity to conclude a contract in the EU is 18 years.[34] Depending on the applicable law, digital service providers must obtain parental permission when children conclude a contract (e.g., an in-app purchase) for the contract to be legally valid, or in certain cases parental permission may be implied depending on the age of the child and the nature of the contract. [35] Consequently, digital service providers could have to verify the age of the contractee to ensure that a contract is legally valid and not void or voidable.[36]

In the case of data protection law, i.e., the GDPR, the minimum age for digital consent as regulated by Article 8 can be determined by Member State law within a range from 13 to 16 years. When children do not yet have the legal capacity to consent to the processing of their personal data, service providers need to obtain parental consent. Therefore, in this case also, age verification is required to know whether a user has reached the minimum age of digital consent to ensure that legally valid consent is obtained for the processing of personal data and, hence, the processing is lawful.[37]

Second, examples of laws protecting children from harmful products or services include prescribing a minimum age for buying harmful products, such as alcohol, cigarettes, and weapons, as well as engaging in harmful services, such as gambling, which regulations are mostly governed by legislation at Member State level.[38] Moreover, particular practices offered as part of a digital service can potentially lead to harm to children. One example is the inclusion of unfair commercial practices in the digital service, such as dark patterns that manipulate children into making in-app purchases.[39] Under the Unfair

---

[34] European Union Agency for Fundamental Rights, (n.d.). *Age of majority*. https://fra.europa.eu/en/publication/2017/mapping-minimum-age-requirements/age-majority#:~:text=The%20age%20of%20majority%20is%2018%20years%20in%20all%20EU,child%20gains%20full%20legal%20capacity.

[35] Cerulli-Harms, A., Münsch, M., Thorun, C., Michaelsen, F., & Hausemer, P. (2020). Loot boxes in online games and their effect on consumers, in particular young consumers. *Publication for the Committee on the Internal Market and Consumer Protection (IMCO), Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg*, *202*. Pg. 33 https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652727/IPOL_STU(2020)652727_EN.pdf.

[36] van der Hof, supra note 24 at 17.

[37] Consent is one of the legal grounds for processing personal data (Article 6 (1) (a) GDPR).

[38] euCONSENT. (Sept 2021). *EU Member State Legal Framework*. Pg. 3-4. https://euconsent.eu/project-deliverables/uCONSENT.eu/project-deliverables/.

[39] van der Hof, S., Lievens, E., Milkaite, I., Verdoodt, V., Hannema, T., & Liefaard, T. (2020). The child's right to protection against economic exploitation in the digital world. *The International Journal of Children's Rights*, *28*(4), 833-859. Pg. 835. https://brill.com/view/journals/chil/28/4/article-p833_833.xml?language=en.

Commercial Practices Directive (UCPD),[40] children are protected as vulnerable consumers and, consequently, are provided with a higher level of protection that must be implemented by service providers.[41]

Similarly, the GDPR provides children and their personal data with a higher level of protection,[42] which, again, can only be implemented when a service provider knows which of their users is a child (unless the high level of protection is afforded to all users). Under the GDPR, it is, e.g., unlawful to target children with personalised advertising,[43] a rule now also endorsed by Article 28 (2) of the Digital Services Act (DSA).[44] Finally, children can also be detrimentally affected due to confrontation with audiovisual harmful content within a digital service, which harm is sought to be regulated in the EU by the Audiovisual Media Services Directive (AVMSD).[45] The AVMSD obliges Member States to ensure that audiovisual media service providers and video-sharing platforms take appropriate measures to protect minors from audiovisual content that "*may impair the[ir] physical, mental or moral development*", including by requiring service providers to use age verification tools in a proportionate manner.[46] The most harmful content (gratuitous violence, pornography, etc.) should be subjected to the strictest measures,[47] such as effective age verification systems.[48] In this regard, the Spanish Data Protection Authority (AEPD) has issued guidance on how age verification systems can be implemented while adhering to data protection obligations, to protect minors from inappropriate

[40] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council, *OJ L 149, 11.6.2005, p. 22–39.*

[41] Unfair commercial practices, which include aggressive commercial practices where advertisements are targeted at children to buy advertised products, are prohibited. See Recital 18, Article 5(1) and Para 28 of Annex I UCPD.

[42] E.g., Recitals 38 and 71 GDPR.

[43] Article 29 Working Party. (27.02.2013). *Opinion 02/2013 on apps on smart devices*. WP 202. Pg. 26. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf.

[44] 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*, OJ L 277, 27.10.2022, p. 1–102.*

[45] 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, *OJ L 303, 28.11.2018, p. 69–92.*

[46] Article 6a and Article 28b AVMSD.

[47] Article 6a and Article 28b (3) AVMSD.

[48] euCONSENT, *supra* note 38 at 7; see also Article 6a (1) and Article 28b (3) (f) AVMSD.

content.[49] Spain's National Markets and Competition Commission (CNMC) is also conducting public consultation by seeking inputs on the criteria required to ensure adequate age verification by video-sharing platforms that host content harmful to children.[50] In Germany, the Commission for the Protection of Minors in the Media (KJM) has established criteria for the evaluation of age verification systems used for preventing children from accessing age-inappropriate content.[51]

A position similar to the AVMSD is present in the UK as well. The UK Online Safety Act 2023 *inter alia* prescribes that platforms ('user-to-user services'[52]) should operate their services by protecting children from harmful content.[53] A higher level of protection is needed for content that is deemed by the state to be most harmful to children ('primary priority content'[54]) and children of all ages are to be prevented from encountering such content, including by employing age verification or age estimation or both.[55] In the context of pornographic content, the UK's Office of Communications (Ofcom) has issued a draft guidance on the implementation of age assurance.[56]

---

[49] Hogan Lovells. (02.01.2024). *Spanish Data Protection Agency's Guidance on age verification*. https://www.engage.hoganlovells.com/knowledgeservices/viewContent.action?key=Ec8teaJ9Vap8ahmeIu1Hl17eOOGbnAEFKCLORG72fHz0%2BNbpi2jDfaB8lgiEyY1JAvAvaah9lF3dzoxprWhI6w%3D%3D&nav=FRbANEucS95NMLRN47z%2BeeOgEFCt8EGQ0qFfoEM4UR4%3D&emailtofriendview=true&freeviewlink=true; AEPD. (Dec 2023). *Decálogo de principios. Verificación de edad y protección de personas menores de edad ante contenidos inadecuados*. https://www.aepd.es/guias/decalogo-principios-verificacion-edad-proteccion-menores.pdf.

[50] Hogan Lovells. (02.01.2024). *Spanish Data Protection Agency's Guidance on age verification*. https://www.engage.hoganlovells.com/knowledgeservices/viewContent.action?key=Ec8teaJ9Vap8ahmeIu1Hl17eOOGbnAEFKCLORG72fHz0%2BNbpi2jDfaB8lgiEyY1JAvAvaah9lF3dzoxprWhI6w%3D%3D&nav=FRbANEucS95NMLRN47z%2BeeOgEFCt8EGQ0qFfoEM4UR4%3D&emailtofriendview=true&freeviewlink=true; CNMC. (n.d.). *PUBLIC CONSULTATION ON THE CRITERIA FOR ENSURING THE APPROPRIATENESS OF AGE VERIFICATION SYSTEMS ON VIDEO-SHARING PLATFORM SERVICES FOR CONTENT THAT IS HARMFUL FOR MINORS*. INF/DTSA/329/23. https://www.cnmc.es/sites/default/files/editor_contenidos/Audiovisual/1_1_INF_DTSA_329_23_Public consultation age verification CNMC Spain_eng.pdf.

[51] KJM. (n.d.). *Supervision*. https://www.kjm-online.de/en/supervision; KJM. (12.05.2022). Kriterien zur Bewertung von Konzepten für Altersverifikationssysteme als Elemente zur Sicherstellung geschlossener Benutzergruppen in Telemedien nach § 4 Abs. 2 S. 2 JMStV. https://www.kjm-online.de/fileadmin/user_upload/KJM/Aufsicht/Technischer_Jugendmedienschutz/AVS-Raster_ueberarbeitet_gueltig_seit_12.05.2022__004_.pdf.

[52] As defined in Section 3(1) UK Online Safety Act 2023.

[53] Section 12(3) UK Online Safety Act 2023.

[54] As per Section 61 UK Online Safety Act 2023, primary priority content means content such as pornographic content, content encouraging or promoting suicide or self-injury or eating disorders and so on.

[55] Section 12(4) UK Online Safety Act 2023.

[56] Ofcom. (05.12.2023). *Guidance on age assurance and other Part 5 duties for service providers publishing pornographic content on online services*. https://www.ofcom.org.uk/__data/assets/pdf_file/0018/272601/guidance-part-5-annexe-2.pdf.

In addition, there are recent measures advanced by countries to generally address online harms caused by social media and other such platforms. For instance, a new law[57] was adopted in France recently which provided for a digital age of majority (15 years) for minors to protect children from harms caused on social media platforms.[58] In essence, users under the age of 15 require consent from parents to register and use such platforms.[59] Compliance with such a stipulation would inevitably require platforms to verify the (minimum) age of users to ascertain whether platforms are required to obtain such consent or not.

3.2. Age assurance as a duty of care

The law may also impose a duty of care regarding the (online) protection of children. An example is the protection of children from harmful content (not being the most harmful content such as gratuitous violence, pornography, etc., see section 3.1). [60] The AVMSD stipulates that children should be protected by proportionate measures from content that has relatively lower risk but may still be harmful.[61] However, such protection measures may not necessitate strict age assurance methods, though the regulatory approach depends on different Member States.[62] Another example of a duty of care is Article 28 DSA, which imposes a duty on online platforms to "*put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors*". Age assurance *may* be a measure to achieve child protection, but it is not mandated by the DSA as the (only) solution.[63] For instance, age assurance could be considered as a potential risk mitigation measure under Article 35 (1) (j) DSA (for very large online platforms and very large online search engines),

[57] French Law no. 2023-566, (07.07.2023).

[58] Le Monde. (29.06.2023). *France requires parental consent for under-15s on social media*. https://www.lemonde.fr/en/france/article/2023/06/29/france-requires-parental-consent-for-under-15s-on-social-media_6039514_7.html.

[59] Nomos. (02.10.2023). *The introduction of a digital age of majority and new obligations for social networks*. https://www.lexology.com/library/detail.aspx?g=c8be7729-5509-40e9-8365-0eb7ebdd3d35.

[60] Similarly, in the UK Online Safety Act 2023, content which is not deemed to be the most harmful, i.e., 'primary priority content', is treated differently. Platforms should protect children from such relatively less harmful content based on their age group and the risk of harm posed, which protection can be by using age assurance; see Section 12(3)(b) and 12 (7) UK Online Safety Act 2023.

[61] Article 6a and 28b AVMSD.

[62] euCONSENT, *supra* note 38 at 7.

[63] Note that when age assurance is implemented to comply with the duty of care in Article 28 DSA, this does not imply an obligation for online platforms "*to process additional personal data in order to assess whether the recipient of the service is a minor*" (see Article 28 (3) DSA).

tailored to the specific risks identified pursuant to Article 34 DSA, which include risks to children.[64]

Ensuring age-appropriate design of (certain functionalities or parts of) digital services for children is another area where age assurance may be relevant, and which may, in itself, be a way to fulfil one's duty of care as a service provider. While a detailed analysis of the sphere of age-appropriate design is outside the scope of this report, it would still be pertinent to touch upon this topic in the context of age assurance. This is because determining what would be age-appropriate design of (a particular functionality or part of) the service with respect to specific groups of users could, for instance, involve ascertaining the age of the users of a platform. Age-appropriate design could also provide users with the option to choose the age or age range corresponding to the online experience they prefer, thus requiring an assessment of whether a given version of the platform matches the age of a user or their preferences. In practise, where platforms ascertain that a user is moving into a higher risk scenario, they may still engage age assurance at certain trigger points, for example when engaging in live chat with an adult or moving from a mixed age setting to an 18+ setting (the latter of which may, depending on the circumstances, also result in a legal obligation for age verification anyway).

It is relevant to mention that the EU's Better Internet for Kids (BIK+) strategy has proposed the creation "*of a comprehensive EU code of conduct on age-appropriate design building on the framework provided in the DSA*" and "*in line with the AVMSD and GDPR*".[65] Various age-appropriate design codes already exist. The UK Information Commissioner's Office (ICO) was the first to issue the Age-Appropriate Design Code[66] (now: Children's Code, AADC) aimed at online service providers, which lays down 15 technology-neutral standards that should be considered by such entities. The third standard in the AADC stipulates that a risk-based approach be adopted to ascertain the age of users unless the standards in the code are applied to all users. A similar position has been adopted by the Data Protection Commissioner (DPC) of Ireland as well.[67] In the United States (US), states such as California have also passed legislation similar to the AADC, i.e., the California Age-Appropriate Design Code of 2022[68] (CAADC). In the US context, such legislations have faced stiff resistance in

[64] Article 34 (1) (d) DSA.

[65] European Commission, *supra* note 7 at 9, 11.

[66] ICO. (17.10.2022). *Age appropriate design: a code of practice for online services*. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/.

[67] DPC, *supra* note 16.

[68] Congressional Research Service. (17.08.2023). *Online Age Verification (Part I): Current Context*. Pg. 1. https://crsreports.congress.gov/product/pdf/LSB/LSB11020.

courtrooms mainly on the grounds of free speech protections. The CAADC was recently injuncted by a federal court while stating that the age assurance requirements of the statute could be invasive to users.[69]

It is pertinent to state that one principle of age-appropriate design as identified by the DPC provides that if the platforms adopt a "*'floor' of protection for all users*", thereby providing a high degree of protection to all users irrespective of whether they are children, then age verification may not be required (for compliance with the DPC's guidelines).[70] Hence, age assurance, again, is not the only solution and what solution is proportionate will also depend on the potential (risk of) harm involved in using the service. However, the reality is that digital services are often not age-appropriate by design in that manner, *inter alia*, because functionalities are not tailored to the rights and well-being of children or do not take into account their vulnerabilities. Hence, protection measures such as age assurance may be necessary for children, though other measures may also be sufficient. In conclusion, age-appropriate design codes and standards aim to make age-appropriateness of (a particular functionality or part of) digital services the default option for all users (including children), which may, on many occasions, require age assurance as a complementary component.

In view of the above, for the second category of cases (as outlined in the present section, age assurance as a duty of care), it is relevant to determine whether age assurance is a necessary measure in the first place. Age verification, in particular, can be an exclusionary measure, i.e., children may be excluded from (parts of) a service, and should therefore be used with caution.[71] Age assurance may not necessarily exclude (certain groups of) children from (parts of) a digital service, though it can also do that, but the question then is whether it leads to the necessary protection of children or whether other protection instruments can be expected to achieve a better result in terms of effectiveness and respecting the rights of the child. For instance, the ICO has stated in its guidance to platforms that self-declaration would not be an adequate age assurance method to demonstrate that children cannot access the platform.[72] This is *inter alia* on account of the fact that it is "*common for*

---

[69] The Verge. (18.09.2023). *Court blocks California's online child safety law*. https://www.theverge.com/2023/9/18/23879489/california-age-appropriate-design-code-act-blocked-unconstitutional-first-amendment-injunction*; NetChoice LLC, v. Rob Bonta*, Case No. 22-cv-08861-BLF, United States District Court, Northern District of California, San Jose Division.

[70] DPC, *supra* note 16 at 6, 16.

[71] 5Rights Foundation, *supra* note 21 at 51.

[72] ICO. (n.d.). *'Likely to be accessed' by children – FAQs, list of factors and case studies.* https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/likely-to-be-accessed-by-children/#threshold.

children to lie about their age to gain access to platforms that appeal to them".[73] So, in this case, this particular form of age assurance does not provide the necessary protection.

In terms of achieving a more child rights-respecting result, and assuming there is no legal obligation for age verification in the given situation, digital service providers can also opt for providing younger users, and potentially their parents, options to tweak or customise their settings. This can enable the settings to be customised in ways that match the wants and needs of children, and in relation to their rights, well-being and healthy or optimal development. Such settings should be accessible and understandable to children and, preferably, standardised across platforms. Such more flexible options can support the rights of children in various ways. They may more adequately reflect the individual needs of a child (even children of similar ages can be very different) in line with their right to appropriate content, by, for example, tailoring content to what a child wants to see while allowing them to avoid unwanted content. Moreover, it provides children, and potentially parents, with more control over their online experiences in line with their participation rights.[74] Technical measures, including age ratings and parental control tools, can be appropriately leveraged to enable such customisation by children and parents.

3.3. Age assurance as a contractual obligation

Even if the law does not impose an obligation of age assurance on digital service providers, they may nevertheless be required to determine whether a user is above a required minimum age or below a required maximum age[75], if there is a contractual stipulation to this effect. For instance, the terms and conditions with the user for access and use of (parts of) the platform may contain such a minimum age, thereby requiring age assurance to be employed. The consequences of non-compliance with such contractual terms will,

[73] GCHQ. (Nov 2020). *VoCO (Verification of Children Online). Phase 2 Report*. Pg. 14. https://www.gov.uk/government/publications/voco-verification-of-children-online-phase-2-report.

[74] The UNCRC contains several rights of children, which rights can be categorised into "*the three Ps*", i.e. children's rights to provision, protection and participation. See Theobald, M. (2019). UN Convention on the Rights of the Child: "Where are we at in recognising children's rights in early childhood, three decades on…?". *International Journal of Early Childhood*, *51*(3), 251-257. Pg. 251. https://doi.org/10.1007/s13158-019-00258-z. E.g., children have a right to education as per Article 28 (provision), children are to be protected from all forms of violence as per Article 19 (protection), and children have a right to freedom of association and peaceful assembly as per Article 15 (participation).

[75] While restricting users on the ground of age usually relates to minimum ages, it cannot be ruled out that maximum ages may be stipulated as well. E.g., to prevent adults from accessing children-only online spaces to combat actions such as sexual grooming. As prescriptions relating to maximum ages are not that common, the present report shall use the terminology minimum age when referring to age-related restrictions.

however, depend on the applicable law. Such scenarios of contractual obligations will also require an assessment of whether age assurance is a necessary measure (similar to what has been discussed in section 3.2), given that age assurance can impact the fundamental freedoms of users, including children.

3.4. Final remarks

Finally, it bears mention that there may be situations where there is no legal or contractual stipulation for age assurance, but a platform still arrives at an assessment that, given the risks posed by the platform to the online safety of children, age assurance is a relevant mitigation measure. For instance, although Article 28 DSA applies only to online platforms, other providers not covered by this provision may also consider complying with this duty of care, for example, because children use the service and may encounter risks there and age assurance may be a relevant mitigation measure. In essence, such voluntary decisions to implement age assurance should also be undertaken after assessing the necessity of the measure as mentioned above. It is also relevant to state that given the diversity of activities, entities and users in the online sphere, there may be overlap between the various ways in which age assurance is legally relevant as described in this section.

Before delving into what requirements ought to be followed by platforms while determining whether age assurance is required and while ascertaining what method of age assurance is to be used, it is pertinent to have a look at the main types of age assurance methods that are present today.

4. Age assurance typologies

There are several methods of age assurance that are present today and still more that may come to fruition in the near future. A brief description of the main types of age assurance that are relevant for consideration for the purposes of the present report are provided below. In the below, we provide a general overview of types of age assurance, and their possible general characteristics and issues. However, the actual characteristics and issues depend on the context and specific design of age assurance methods.

4.1. Overview, characteristics and issues

4.1.1. Self-declaration

As stated above (section 2), this is a category of age assurance which consists of methods that rely on the individual to supply their age or confirm their age range, without providing any evidence to prove such declaration.[76] Self-declaration methods reduce (and sometimes do not require) personal data from being provided to platforms by users for the purpose of age assurance.[77] However, self-declaration provides a very low level of assurance, as it is a trust-based method that can be easily circumvented, [78] as can be seen in the example below (fig. 1). The level of assurance from self-declaration can be slightly increased through the design of the self-declaration process, e.g., if the date of birth entered is below the minimum age, then the platform can deny access and block consequent attempts from that IP address even if the date of birth is changed thereafter.[79] In practice, such additional assurance measures can also be circumvented relatively easily, e.g., by logging in through a virtual proxy network (VPN) or a different browser.[80]

[76] ICO, *supra* note 15 at 14.

[77] UNICEF. (Apr 2021). *Digital Age Assurance Tools and Children's Rights Online across the Globe: A Discussion Paper*. Pg. 23. https://c-fam.org/wp-content/uploads/Digital-Age-Assurance-Tools-and-Childrens-Rights-Online-across-the-Globe.pdf.

[78] ICO, *supra* note 15 at 14.

[79] 5Rights Foundation, *supra* note 21 at 27.

[80] van der Hof, *supra* note 24 at 41.

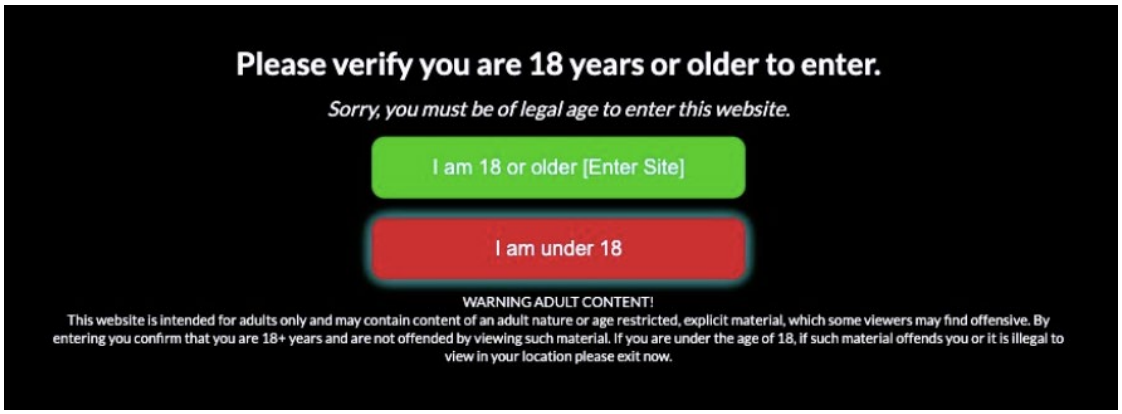


Fig. 1: Example of self-declaration as age assurance method; © 5Star Plugins (n.d.) https://5starplugins.com/easy-website-age-verification/#standard

4.1.2. Hard identifiers

This is an age verification method where users provide verified identity documents (e.g., passports) to prove their age.[81] The identity document is usually submitted by uploading a scan or image of the document or – to raise the assurance level – through live video verification of the document by a human agent.[82] Further, several Member States have electronic identification documents at the national level.[83] At times, information present in such national electronic identity databases is allowed to be accessed by service providers for age verification purposes (e.g., Spain and Denmark allow gambling operators to access such databases).[84]

Hard identifiers generally provide a high level of assurance when it is ensured that the identification document belongs to the user themself.[85] However, many children do not have official identification[86] and using this method can hence lead to their digital exclusion. Further, this method may have a disproportionate impact on the privacy of all users.[87] It bears mention that at the EU level, the proposed European Digital Identity regulation (eID proposal)[88] envisages a

[81] 5Rights Foundation, *supra* note 21 at 28.

[82] euCONSENT. (02.01.2022). *D2.2 EU Methods for AVMSD and GDPR Compliance Report*. Pg. 8. https://euCONSENT.eu/project-deliverables/.

[83] British Standards Institution. (31.03.2018). *PAS 1296:2018 Online age checking. Provision and use of online age check services. Code of Practice*. Pg. 36-37.

[84] UNICEF, *supra* note 77 at 16; *Ibid* at 37.

[85] 5Rights Foundation, *supra* note 21 at 28.

[86] UNICEF, *supra* note 77 at 23.

[87] ICO, *supra* note 66 at 34.

[88] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, COM/2021/281 final, (03.06.2021).

mechanism based on national laws to allow citizens to use digital identity wallets "*to prove their age without disclosing other personal data*".[89] However, for the digital identity wallet to play a significant role in interoperable EU-wide age assurance, all Member States would have to proceed to issue eIDAS (electronic Identification, Authentication and Trust Services) credentials to minors.

4.1.3. Credit cards

Credit card data can be used to verify that a user is above 18 years old, provided that credit cards are issued only to adults in a given jurisdiction.[90] Generally, users provide their name and credit card details, which are checked against a financial database to confirm the validity of the card,[91] and at times a small payment (e.g., 0.01 €), or payment authorisation, is effected to ensure certainty.[92] This method can provide effective age verification in countries where only individuals above 18 are allowed to be issued credit cards.[93] However, this method can lead to the exclusion of adults who do not have such credit cards, and inequalities in access to credit cards on the basis of income, ethnicity and age have also been noticed in studies.[94] Further, apart from the privacy and security concerns that are ostensibly present in providing such financial information, children can potentially circumvent this verification by obtaining an adult's credit card.[95]

4.1.4. Self-sovereign identity

There are methods proposed to use decentralised technologies such as blockchain for creating digital identities of users, which can also be used for age verification purposes.[96] Such methods can increase the user's control over the data and reduce the influence of governments and private companies in age

[89] European Commission, *supra* note 7 at 3-4.

[90] euCONSENT, *supra* note 82 at 9.

[91] *Id.*

[92] European Parliamentary Research Service, *supra* note 16 at 1.

[93] euCONSENT, *supra* note 82 at 9.

[94] US Federal Reserve System. (May 2023). *Economic Well-Being of U.S. Households in 2022*. Pg. 44, 45. https://www.federalreserve.gov/publications/files/2022-report-economic-well-being-us-households-202305.pdf.

[95] UNICEF, *supra* note 77 at 23.

[96] PricewaterhouseCoopers. (2019). *Blockchain and Digital Identity: the path to Self Sovereign Identity*. https://www.pwc.com/it/it/publications/assets/docs/blockchain-and-digital-identity.pdf; Devi, S., Kotian, S., Kumavat, M., & Patel, D. (2022). Digital Identity Management System Using Blockchain. *Available at SSRN 4127356*.

verification processes.[97] However, the practical adoption of such digital identities may be difficult due to lack of standardisation and restricted user adoption.[98]

4.1.5. Account holder confirmation

This method of age assurance, which is also called vouching, occurs when the platform relies on the confirmation of one or more existing verified account holders. In essence, the current account holder provides an assurance to the platform that another user is of the required age to use the platform.[99] For instance, an (alleged or verified) adult using a video streaming service may create a user profile for their child to use the service in an age-appropriate way (in which case the method overlaps with parental control).[100] The level of age assurance in this method thus depends on the integrity of the existing account holder, and this method provides platforms with an avenue to provide age-appropriate services to a child.[101] However, this method raises concerns regarding the child's privacy (including from their parents or guardians) and could also lead to the exclusion of children and adults who cannot obtain such confirmation from an existing account holder.[102] This is *inter alia* because children (particularly older children) could want access to online services without parental involvement, e.g., for obtaining sexual health services.[103]

4.1.6. Cross-platform authentication

Existing user accounts on large platforms, such as Google, Apple, or Microsoft, could be used to authenticate the age of a user. Briefly put, these platforms themselves verify the age of the users through any of the methods mentioned above and then authenticate the age of the user when the user has to access new products or services.[104] This can be by way of solutions on user devices

---

[97] UNICEF, *supra* note 77 at 22.

[98] Finance Magnates. (13.03.2023). *Identity on the Blockchain: Building a More Secure Future*. https://www.financemagnates.com/cryptocurrency/education-centre/identity-on-the-blockchain-building-a-more-secure-future/.

[99] ICO, *supra* note 66 at 34.

[100] euCONSENT, *supra* note 82 at 11.

[101] 5Rights Foundation, *supra* note 21 at 40.

[102] *Ibid* at 41.

[103] *Id*.

[104] ICO. (n.d.). *The ICO's response to the Call for Evidence and roundtables on age assurance*. https://ico.org.uk/media/about-the-ico/consultations/4023900/20230203-response-to-aa-cfe-and-roundtables-v1_1.pdf; *Ibid* at 33-34.

(e.g., Google Android, Apple iOS)[105] or through user accounts (e.g., Facebook, X (formerly Twitter).[106] However, the level of assurance in this method is contingent on the initial assurance method used by the large platform, and there is also no sufficient clarity on the data sharing that occurs in such cross-platform authentication thereby raising privacy concerns.[107] Additionally, making such a method of age assurance widespread would put these larger platforms in an even more powerful position regarding how users interact with the internet, and "*may further entrench their market dominance*".[108] Furthermore, as mentioned previously, the level of assurance for this method depends on the original assurance methods used by the large platforms, which assurance activities would conceivably have been undertaken by the large platforms in the context of their own digital services. Thus, the risks posed by the new products or services may have no co-relation with the assurance activities done by the large platforms, thereby potentially resulting in there not being sufficient assurance level or disproportionately high assurance level, as the case may be. Moreover, it does not necessarily mean that children are no longer at risk online because they may, for instance, share devices or user accounts with older children or adults. Finally, it is the responsibility of digital service providers to determine, for example through a risk assessment, what are the most appropriate and adequate protection measures (including age assurance), for their specific service, or functionalities and components thereof.

4.1.7. Facial age estimation

This is an age estimation method where artificial intelligence (AI) is used to analyse the facial features of a person, either through sharing of a live image or video or by analysing an existing picture, to estimate the age of a person.[109] There are several platforms which employ this technology as well as third-party service providers that provide facial age estimation services. The level of assurance provided by facial age estimation methods would depend on the technology used and ranges from very low to very high.[110] In fact, the National Institute of Standards and Technology (NIST) in the US is conducting an evaluation of facial age estimation technologies, including about the accuracy and efficiency of the software algorithms that are utilised.[111]

---

[105] ICO, *supra* note 104.

[106] 5Rights Foundation, *supra* note 21 at 33-34.

[107] *Ibid* at 34.

[108] *Id*.

[109] euCONSENT, *supra* note 82 at 10.

[110] 5Rights Foundation, *supra* note 21 at 31.

[111] NIST. (n.d.). *Face Analysis Technology Evaluation (FATE) Age Estimation & Verification*. https://pages.nist.gov/frvt/html/frvt_age_estimation.html.

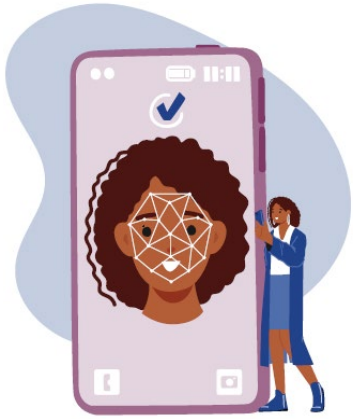


Fig. 2: An illustration of facial estimation; © eSafety Commissioner, Australia[112]

One of the benefits of this method is that users find it to be "*easy, fast and less invasive compared to the other options*", and the method was thus found to be the most popular option by participants in a study conducted by the euCONSENT project.[113] However, depending on its design, this method may still raise privacy issues, including regarding the processing of special categories of personal data, as biometric data can potentially be used for age estimation.[114] Because of the reliance on bodily and physical characteristics that are unique to individuals, and the potential to estimate traits other than age (again depending on the design of the system), it may therefore be a more intrusive and sensitive technology. [115] In a given context, it may still be acceptable to users. The use of biometric data can, however, have a normalising effect of such technologies, and surveillance more generally, on users, including children.[116] Further, depending on the technology used, there could be potential issues associated with biases in AI algorithms, lack of transparency and accuracy of such technologies, especially also with respect to children.[117] Certain types of biometric age estimation has been assessed

[112] eSafety Commissioner, Australia. (Mar 2023). *Roadmap for age verification and complementary measures to prevent and mitigate harms to children from online pornography*. Pg. 20. https://www.esafety.gov.au/sites/default/files/2023-08/Roadmap-for-age-verification_2.pdf.

[113] euCONSENT. (08.05.2022). *D6.3.3 Pilot Execution Report*. Pg. 49. https://euconsent.eu/project-deliverables/.

[114] European Parliamentary Research Service, *supra* note 16 at 1. However, it is not necessary that special categories of personal data are processed by facial age estimation technologies: see, ICO. (April 2022). *Regulatory Sandbox Final Report: Yoti*. Pg. 10. https://ico.org.uk/media/for-organisations/documents/4020427/yoti-sandbox-exit_report_20220522.pdf.

[115] Paik, S., Mays, K. K., & Katz, J. E. (2022). Invasive Yet Inevitable? Privacy Normalization Trends in Biometric Technology. *Social Media+ Society*, *8*(4), 20563051221129147.

[116] *Ibid* at 14.

[117] Congressional Research Service. (23.03.2023). *Challenges with Identifying Minors Online*. Pg. 2.

positively by the German KJM.[118] The French Commission Nationale Informatique & Libertés (CNIL) has stated that facial age estimation, through an independent third party and without facial recognition, can be acceptable until adequate new ways of age assurance become available.[119]

An added concern is the potential to further use the data emanating from facial analysis[120] and make it available for biometric technologies such as facial recognition.[121] Facial recognition can be used for commercial or political surveillance.[122] Children are at a graver risk in these cases since they are exposed to such technologies from a young age and throughout the course of their lives. [123] Thus, they will have to face the consequences of the high volume of data collated by such technologies, and for a significantly longer time than adults.

4.1.8. Behavioural profiling

Analysing the profiling data of users based on their activity online by employing AI could provide an estimate of users' age.[124] For instance, this analysis could include scrutiny of browsing history, user-generated content, purchases, and so on.[125] The level of assurance for this method depends on the quality of the dataset that is used to train the AI.[126] This method may help overcome the risk

https://crsreports.congress.gov/product/pdf/IN/IN12055#:~:text=Potential%20Challenges%20with%20Identifying%20Minors,as%20those%20younger%20than%2013; 5Rights Foundation, *supra* note 21 at 30.

[118] KJM. (24.05.2022). *KJM bewertet Altersverifikationssysteme mit biometrischer Alterskontrolle positiv*. https://www.kjm-online.de/service/pressemitteilungen/meldung/kjm-bewertet-altersverifikationssysteme-mit-biometrischer-alterskontrolle-positiv.

[119] CNIL. (21.02.2023). *Contrôle de l'âge pour l'accès aux sites pornographiques*. https://www.cnil.fr/fr/controle-de-lage-pour-lacces-aux-sites-pornographiques.

[120] Facial analysis is the method to analyse facial features of an individual for purposes such as age, gender, emotion estimation, etc. Facial age estimation is thus a subset of facial analysis.

[121] Facial recognition is the method of using software to analyse the facial features of an individual and identify the individual or verify their identity and is different from facial analysis. See TechTarget. (n.d.). *facial recognition*. https://www.techtarget.com/searchenterpriseai/definition/facial-recognition; NIST. (20.09.2023). *What's Wrong With This Picture? NIST Face Analysis Program Helps to Find Answers*. https://www.nist.gov/news-events/news/2023/09/whats-wrong-picture-nist-face-analysis-program-helps-find-answers.

[122] UNICEF, *supra* note 77 at 41.

[123] UNICEF, *supra* note 77 at 19.

[124] ICO, *supra* note 66 at 34.

[125] European Parliamentary Research Service, *supra* note 16 at 1.

[126] eSafety Commissioner, Australia. (Aug 2023). *Roadmap for age verification and complementary measures to prevent and mitigate harms to children from online*

of excluding children from accessing online services on account of them not having official identification or a parent/guardian who can confirm their age.[127] However, this method raises a major concern for the privacy of all users, and particularly children, and could amount to unwanted data collection and surveillance.[128]

Children may also be incorrectly categorised and may be wrongly allowed access or prevented access to platforms because such profiling is premised on the assumption that the data relating to online behaviour is reflective of a user's age. However, the data used to make such behavioural predictions may not be accurate (e.g., one user account may be used by several persons), and such inaccuracies could also result in discrimination.[129] In addition, such a method raises issues of non-transparency as little is known of how companies "*differentiate behavioural analytics to determine age across countries and contexts*".[130]

4.1.9. Capacity-testing

This is a method where the platform estimates a user's age by testing their aptitude or capacity.[131] For instance, children may be required to take assessments, such as language tests or solving puzzles, to gauge their age.[132] This is a low-assurance but privacy-protective way of age estimation.[133] Such tools may have limited accuracy because a person's aptitude may not be reflective of their biological age.[134] Further, such assessments can be affected by factors such as "*accents, low language fluency or disability, also potentially creating barriers to inclusion*".[135]

pornography. Pg. 153. https://www.esafety.gov.au/sites/default/files/2023-08/Age-verification-background-report.pdf.

[127] UNICEF, *supra* note 77 at 28.

[128] 5Rights Foundation, *supra* note 21 at 33.

[129] UNICEF, *supra* note 77 at 30.

[130] *Ibid* at 29.

[131] 5Rights Foundation, *supra* note 21 at 33.

[132] *Id.*

[133] van der Hof, S., & Ouburg, S. (2022). 'We Take Your Word for It'-A Review of Methods of Age Verification and Parental Consent in Digital Services. *Eur. Data Prot. L. Rev.*, *8*, 61. Pg. 65. https://edpl.lexxion.eu/article/EDPL/2022/1/10.

[134] eSafety Commissioner, Australia, *supra* note 112 at 19.

[135] *Id.*

4.1.10. Third-party age assurance services

There are third-party age assurance providers that are used by platforms to provide an assurance of age or to confirm the identity of the users.[136] The methods used by these third parties themselves vary and could involve a combination of the methods mentioned above, which would, in turn, determine the level of assurance. Such a method may, for example, include issuance of age tokens specifying the age or age range of the users to verify whether a user is above a certain minimum age.[137] The main benefit of using a third-party service provider is that the quantum of personal data collected by the platforms themselves is significantly reduced, as only the age or age attribute, or a "*yes*" or "*no*" response regarding the sufficiency of a user's age is provided to the platform.[138]

That being said, an issue associated with this method is the privacy concerns emanating from the data processed by such third parties themselves, including the data pertaining to websites or platforms accessed by the users.[139] A way to resolve such privacy concerns has been explored by the use of zero-knowledge proof methods, i.e., a process employing cryptology whereby individuals can prove their age (without providing any other information) in a privacy-friendly manner by utilising an independent third-party exchange that acts as a medium between the platforms and the third-party age assurance providers.[140] Such an exchange immediately deletes the data of the user after age confirmation is relayed from the third-party provider to the platform.[141] In this regard, the CNIL in France has recommended that use of a trusted independent third party is the most privacy-friendly way to conduct age verification.[142] CNIL has also conducted demonstrations of the technical viability of such zero-knowledge proof methods.[143] Another example of a privacy-friendly third-party age verification service is the open-source portal Yivi (formerly IRMA), offered by the Privacy by Design Foundation, which facilitates the processing of the data (e.g., an age token) on the device of the user in a decentralised manner.[144] Further, in Spain, an age verification technology that aims to be privacy-friendly while

---

[136] 5Rights Foundation, *supra* note 21 at 35.

[137] *Ibid* at 35-39.

[138] ICO, *supra* note 66 at 34.

[139] UNICEF, *supra* note 77 at 31.

[140] eSafety Commissioner, Australia, *supra* note 126 at 174.

[141] *Ibid* at 175.

[142] CNIL. (22.09.2022). *Online age verification: balancing privacy and the protection of minors*. https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors.

[143] *Id*.

[144] Privacy by Design Foundation. (n.d.). *About IRMA*. https://privacybydesign.foundation/irma-en/; van der Hof, *supra* note 24 at 24.

preventing children from accessing inappropriate content is being developed by the Royal Spanish Mint in conjunction with AEPD's recommendations.[145]

4.2. Relevant cross-cutting aspects

Given the above background, it would be important at this juncture to mention certain aspects regarding the various types of age assurance. First, the above methods are not an exhaustive list of age assurance methods present today and methods such as checking age against data held by entities including banks, mobile phone operators,[146] and credit reference agencies[147] are also used in certain countries. Other age assurance methods, including estimation techniques using voice analysis, hand geometry and natural language processing, could also become prominent in the future.[148] Such estimation techniques are likely to have some of the same issues as those associated with facial age estimation and behavioural profiling. It also bears mention that platforms may use a combination of age assurance methods instead of relying on any one method.[149] For instance, self-declaration can be used in combination with facial age estimation to provide a higher level of assurance.[150]

Second, digital service providers may use the services of third parties for implementing age assurance, by engaging third parties for age assurance services (section 4.1.10), by using third-party algorithms for behavioural profiling (section 4.1.8), etc. The liabilities associated with ensuring age assurance in such situations would inevitably depend on the applicable legal regime and the facts involved. For instance, Article 28 DSA tasks online platforms themselves with protecting children on their platforms. Article 28b AVMSD obliges video-sharing platforms to take measures to protect minors against harmful content, which may include the use of age assurance systems. Under the GDPR, as regards the personal data processed for age assurance, it could be a controller to processer relationship between the digital service providers and third parties, or the two entities could be joint controllers, and so

[145] Reuters. (14.12.2023). *Spain readies age-checking tech to protect children from adult online content*. https://www.reuters.com/world/europe/spain-readies-age-checking-tech-protect-children-adult-online-content-2023-12-14/.

[146] 5Rights Foundation. (Oct 2021). *But how do they know it is a child?. Age Assurance in the Digital World*. Pg. 26. https://5rightsfoundation.com/uploads/But_How_Do_They_Know_It_is_a_Child.pdf; euCONSENT. (02.01.2022). *D2.2 EU Methods for AVMSD and GDPR Compliance Report*. Pg. 9, 10. https://euCONSENT.eu/project-deliverables/.

[147] euCONSENT. (02.01.2022). *D2.2 EU Methods for AVMSD and GDPR Compliance Report*. Pg. 9. https://euCONSENT.eu/project-deliverables/.

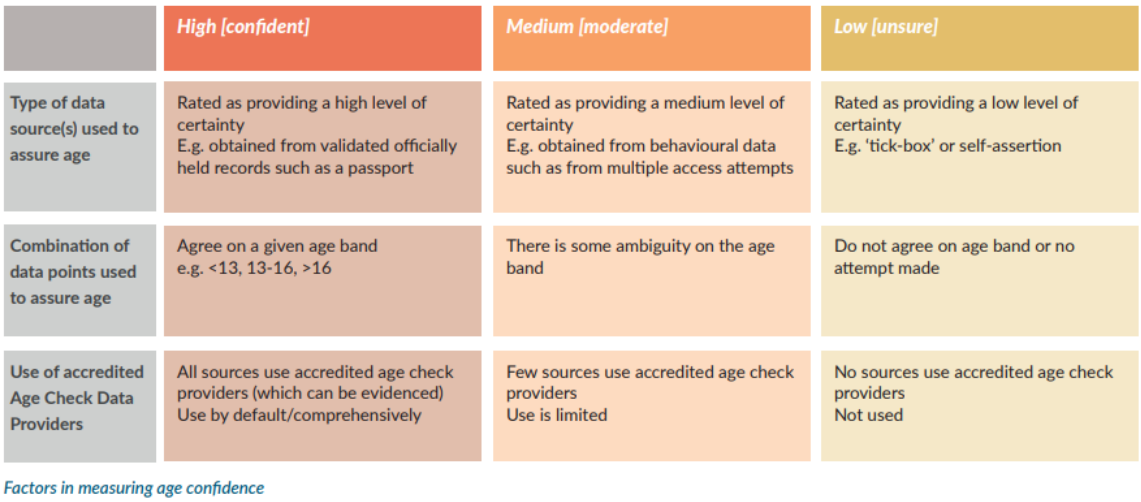
[148] ICO, *supra* note 15 at 37; euCONSENT, *supra* note 82 at 11.

[149] 5Rights Foundation, *supra* note 21 at 45.

[150] *Ibid* at 27.

on, depending on the nature of their arrangement. Thus, the primary responsibility for ensuring appropriate age assurance will be on the digital service providers themselves. However, ultimately, it is for the policymakers and regulators to impose accountability on the relevant party based on the context at hand.

Third, with regard to the certainty or assurance levels of age assurance methods, there are various views present in the literature regarding the assurance levels of particular methods.[151] There have also been initiatives to propose a mechanism to determine the confidence one can have regarding the accuracy of given age assurance methods. In this regard, Government Communications Headquarters UK (GCHQ) proposes a three-level low-medium-high confidence model (fig. 3)[152], the International Organisation for Standardization's (ISO) working draft on age assurance proposes a five-level zero-basic-standard-enhanced-strict confidence model (fig. 4),[153] and so on. Further clarity may be achieved regarding this aspect as more work is undertaken by organisations on age assurance in the future (see section 5.9).



	High [confident]	*Medium [moderate]*	*Low [unsure]*
Type of data source(s) used to assure age	Rated as providing a high level of certainty E.g. obtained from validated officially held records such as a passport	Rated as providing a medium level of certainty E.g. obtained from behavioural data such as from multiple access attempts	Rated as providing a low level of certainty E.g. 'tick-box' or self-assertion
Combination of data points used to assure age	Agree on a given age band e.g. <13, 13-16, >16	There is some ambiguity on the age band	Do not agree on age band or no attempt made
Use of accredited Age Check Data Providers	All sources use accredited age check providers (which can be evidenced) Use by default/comprehensively	Few sources use accredited age check providers Use is limited	No sources use accredited age check providers Not used

Factors in measuring age confidence

Fig. 3: Model proposed by GCHQ for confidence in age assurance methods

[151] E.g. 5Rights Foundation, *supra* note 21; UNICEF, *supra* note 77; eSafety Commissioner, Australia, *supra* note 126.

[152] GCHQ, *supra* note 73 at 18-19.

[153] ISO. (Nov 2021). *ISO Working Draft Age Assurance Systems Standard*. Pg. 13-16. https://euconsent.eu/download/iso-working-draft-age-assurance-systems-standard/.

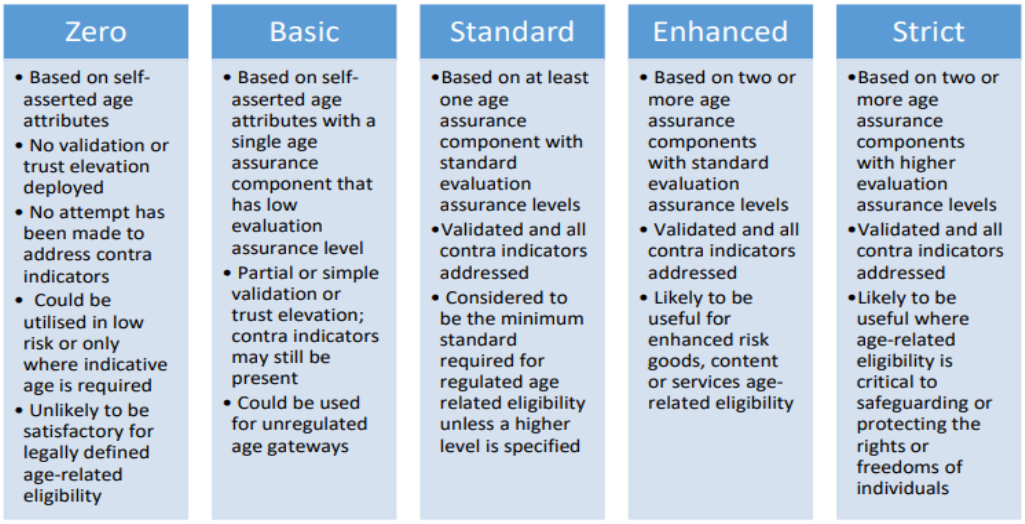


Fig. 4: Model proposed by ISO for confidence in age assurance methods

5. Age assurance requirements

Whether it be for ascertaining if age verification is legally required or for determining which method of age assurance to employ, certain requirements ought to be present to ensure that age assurance is done in an optimal manner. At the same, it must be acknowledged that there are significant challenges and tensions to be combated to achieve these requirements for age assurance systems. It would thus be useful to analyse some of the salient requirements that age assurance methods should have, along with certain corresponding challenges in achieving such requirements. These requirements are (1) Proportionality; (2) Privacy; (3) Security; (4) Accuracy and effectiveness; (5) Functionality and ease of use; (6) Inclusivity and non-discrimination; (7) Furthering participation and access; (8) Transparency and accountability; (9) Notification, challenge, and redressal mechanisms; and (10) Hearing the views of children.

5.1. Proportionality

This is a basic requirement that can play a role in satisfying the other requirements in this section. The principle of proportionality is a fundamental principle when limiting the rights of EU citizens, including children. In the present context, proportionality requires that a balance be struck between (a) the means used to achieve the intended objective and (b) its impact on the limitation of the rights of persons.[154] Part of the proportionality test is to assess whether, of all the available measures that can achieve the intended purpose, the particular measure interferes the least with the rights of users, including children.

In the contexts mentioned above (see section 3), where age assurance or verification is relevant, a solution will have to be found that meets the principle of proportionality. In cases where the law imposes a duty of care regarding the protection of children (as discussed in section 3.2) or where there is a contractual obligation to control the age of users (as discussed in section 3.3) or where such voluntary decisions are made (as discussed in section 3.4), the principle of proportionality plays a role at two – interrelated – levels. In cases where age verification is a requirement in the law (as discussed in section 3.1), only the second level is relevant.

At the first level, it is necessary to analyse *whether age assurance is an effective means of achieving the objective* – i.e., age-appropriate access to

[154] European Data Protection Supervisor. (n.d.). *Necessity & Proportionality*. https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en.

goods and services while maintaining the online protection of the rights and well-being of children. In particular, it must be determined whether age assurance can effectively protect children from the (potential) risks of a digital service while holistically respecting children's rights. That protection may require different measures for different groups of children. The evolving capacities of children under Article 5 UNCRC play an important role here. If it is determined that age assurance is an effective means of both age-appropriate access to goods and services and protecting (certain groups of) children given the (potential) online risks involved, it should be determined whether age assurance is the least invasive way in terms of interference with the rights of users, including children, or if there is a way that is equally proportionate but less invasive. Invasiveness can involve various aspects, including privacy, inclusiveness, user autonomy and security. Invasiveness thus relates to the other requirements mapped in this section of the report.

At the second level, an investigation of *which method of age assurance* or, in particular, age verification is appropriate to implement in the digital service should take place. In cases where the law (see section 3.1) requires a minimum age, thus necessitating age assurance, or age verification in particular, only the examination of potential method(s) of age assurance needs to be done. The method (or a combination of methods) of age assurance should be determined in accordance with the principle of proportionality. Again, this requires an analysis of whether the method (or a combination of methods) achieve the objective (i.e., enabling age-appropriate access and the online protection of the rights and well-being of the child) and, if so, whether it is the most appropriate and least invasive method (or combination of methods) given the other requirements discussed in this section below.

In practically implementing this requirement, a risk-based framework is often suggested in the literature.[155] In this regard, the assurance level required from age assurance systems should be proportionate to the (potential) risk or harm posed to children by the given product or service.[156] This is why higher levels of assurance are demanded for high-risk products or services. For instance, age assurance for preventing children from accessing extreme violence or pornographic content would require methods that have the highest standards of assurance and accuracy.[157] However, attention must be paid to ensure that the presence of risk is not used as a justification to simply block children from platforms or to use age assurance tools that are invasive, without exploring the proportionality requirement.

---

[155] CEN, *supra* note 12 at 27; 5Rights Foundation, *supra* note 21 at 48-49; DPC, *supra* note 16 at 46-47.

[156] Family Online Safety Institute. (July 2023). *Coming to Terms with Age Assurance*. Pg. 6. https://www.fosi.org/policy-research/coming-to-terms-with-age-assurance.

[157] 5Rights Foundation, *supra* note 21 at 49.

Challenge: Difficulty in determining what is proportional
There is no consensus on what the different risks faced by children of different age categories online are,[158] thus complicating the assessment of what would be proportional in different scenarios. Further, the diversity of the online industry, which consists of a variety of platforms, service providers, online sales portals, etc., makes it difficult to formulate common yardsticks for proportionality.
Potential solutions
Conducting a child rights impact assessment (CRIA) could be a helpful method to understand what could be proportional in specific contexts. Digital service providers would be best placed to ascertain the potential risks and harms to children, alongside their rights and well-being from their services, and this should be duly accounted for in the CRIA. Further, continued discussions and studies by academia, regulators and private entities on the various risks faced by children online and the assurance levels required for particular risks (given the extant technologies) would be helpful in this regard.

5.2. Privacy

Age assurance methods may involve the processing of personal or sensitive data of users (including minors)[159] and age assurance providers must then be GDPR compliant. In this regard, regulators such as the UK's ICO and the Irish DPC have clearly stated that data protection principles as enshrined in Article 5 GDPR (data minimisation, accuracy, storage limitation, etc.) ought to be paid due consideration while employing age assurance.[160] Also, Article 28 (3) DSA provides that protective measures that include assessing whether a user is a child should not lead to the processing of additional personal data. Article 6a (2) AVMSD establishes that the personal data of minors collected or otherwise generated by media service providers cannot be processed for commercial purposes. If biometric data is used, then conditions for processing of special categories of data as provided in Article 9 GDPR may also need to be met.[161]

[158] Family Online Safety Institute, *supra* note 156 at 6. See, however, more generally, the OECD online risk classification in: OECD, *supra* note 2.

[159] Brennen, S., & Perault, M. (2023). Keeping Kids Safe Online: How Should Policymakers Approach Age Verification?. *The Center for Growth and Opportunity*. Pg. 8. https://www.thecgo.org/research/keeping-kids-safe-online-how-should-policymakers-approach-age-verification/.

[160] ICO, *supra* note 15 at 20-29; DPC, *supra* note 16 at 48.

[161] ICO, *supra* note 15 at 29.

Challenge: Age assurance and the impact on privacy

Privacy concerns on account of age assurance can *inter alia* occur in two manners:

(a) The increased processing of personal data for age assurance can lead to unauthorised disclosure of data (e.g., due to data breaches) and can also result in platforms and data brokers using the data for other purposes such as targeted advertisements, sale of data, etc.[162]

(b) Age assurance may additionally impact the right to intellectual privacy (access to spaces to read, think and discuss free from surveillance) and, thus, freedom of expression.[163] In fact, organisations such as Electronic Frontiers Foundation (EFF) have strongly opposed age verification mandates while arguing that there is no accurate and privacy-protective age assurance method available at present.[164] EFF has argued that age verification could lead to online surveillance and derogation of anonymity online.[165]

Potential solutions

Implementing age assurance while adhering to principles such as privacy and safety by design[166] should be the aim of age assurance providers. Further, age assurance should not be used by companies as a "*cover for their aggressive data collection practices*".[167]

As regards anonymity and freedom of expression, while restrictions on free speech are viewed more seriously in jurisdictions like the US[168] than the EU, it is still an issue that merits serious consideration in the EU. This is because anonymity online could bolster freedom of expression and (intellectual) privacy and could protect from censorship and surveillance.[169] Thus, while eroding anonymity through age assurance to regulate harmful or illegal content may not always be completely avoidable, this should be done with sufficient safeguards. A balance needs to be found between the object sought to be achieved and the rights that are being limited, and as aforementioned, a proportionate approach is necessary.

---

[162] Brennen, *supra* note 159 at 8.

[163] Richards, N. (2015). *Intellectual privacy: Rethinking civil liberties in the digital age*. Oxford University Press, USA.

[164] EFF. (05.09.2023). *UK Online Safety Bill Will Mandate Dangerous Age Verification for Much of the Web*. https://www.eff.org/deeplinks/2023/09/uk-online-safety-bill-will-mandate-dangerous-age-verification-much-web.

[165] EFF. (10.03.2023). *Age Verification Mandates Would Undermine Anonymity Online*. https://www.eff.org/deeplinks/2023/03/age-verification-mandates-would-undermine-anonymity-online.

[166] euCONSENT. (Sept 2021). *Understanding of user needs and problems: A rapid evidence review of age assurance and parental controls*. Pg. 7. https://euCONSENT.eu/project-deliverables/.

[167] 5Rights Foundation, *supra* note 21 at 48.

5.3. Security

As stated above, age assurance could involve the processing of personal data, and it is therefore important that age assurance systems are secure and prevent unauthorised access to the data so processed.[170] Age assurance systems must also have sufficient cybersecurity measures in order to ensure that their functioning is not compromised to the detriment of children, other users, and platforms. From a compliance perspective, apart from the security considerations that must be implemented as per the GDPR,[171] age assurance providers may also have to adhere to the essential cybersecurity requirements prescribed by the proposed Cyber Resilience Act, 2022 (CRA)[172] in the future.

Challenge: Sophistication of cyberattacks

Achieving a fully secure age assurance system may be practically difficult. This is *inter alia* due to the increasing frequency, sophistication and impact of cyberattacks.[173] For instance, as per an estimate, the annual worldwide cost of cybercrime, owing to successful cyberattacks effected on hardware and software products, was EUR 5.5 trillion in 2021,[174] reflective of the magnitude of this problem.

Potential solutions

Age assurance providers should expend sufficient resources and manpower to stay ahead of the curve when it comes to ensuring optimal cybersecurity measures. Adherence to industry standards on cybersecurity measures such as ISO 27001[175] and 27002[176], and staying up to date with guidance

[168] Congressional Research Service. (17.08.2023). *Online Age Verification (Part II): Constitutional Background*. https://crsreports.congress.gov/product/pdf/LSB/LSB11021.

[169] Bodle, R. (2013). The ethics of online anonymity or Zuckerberg vs. "Moot". *Acm Sigcas Computers and Society*, *43*(1), 22-35. Pg. 24. https://dl.acm.org/doi/10.1145/2505414.2505417.

[170] CEN, *supra* note 12 at 27.

[171] Article 32 GDPR states that controllers and processors shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account several factors, including the nature, scope, context and purposes of the data processed.

[172] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM(2022) 454 final, (15.09.2022).

[173] ENISA. (Oct 2021). *ENISA THREAT LANDSCAPE 2021*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021?v2=1.

[174] Pg. 1 CRA.

[175] ISO and IEC. (2013). *Information technology — Security techniques — Information security management systems — Requirements*. ISO/IEC 27001:2013(E).

[176] ISO and IEC. (2013). *Information technology — Security techniques — Code of practice for information security controls*. ISO/IEC 27002:2013(E).

provided by agencies such as the European Union Agency for Cybersecurity (ENISA), could be useful in this regard. Compliance with the principle of data minimisation and thus reducing the data susceptible to cyberattacks could also be helpful and is a legal requirement in the EU.

5.4. Accuracy and effectiveness

Accuracy of age assurance methods is a fundamental requirement as, without sufficient assurance levels, the age assurance method will not be effective in mitigating the risks posed to children. The more accurate the age assurance method is, the lesser the likelihood for children to access platforms that they are not allowed to or for users not to be granted access to a platform despite being of sufficient age. In fact, lack of accuracy is one of the main criticisms faced by self-declaration methods,[177] since children are not always providing their true age when they want to access certain platforms.[178] Thus, platforms should not use self-declaration under the presumption that users will be truthful about their age. Hence, self-declaration is, by itself, not a proportionate solution when age verification is legally mandated or the nature of the platform presents high risks to children.[179] Further, when third-party age assurance providers are engaged by platforms, it could be useful to ascertain the accuracy of such third parties by requiring independent certification or validation regarding their accuracy.[180]

Challenge #1: Enhancing accuracy could impact privacy

The accuracy of the age assurance method employed could have an inverse relation to the privacy rights of users.[181] For instance, the use of hard identifiers could provide high accuracy but could also be the most invasive.[182] Conversely, self-declaration may provide low accuracy but can be performed without requiring much data from the users.

Potential solutions

This is an aspect to be paid due consideration so that the principle of necessity and proportionality can play a role in finding the right balance between these requirements. Incorporating privacy-friendly processes in age

[177] CNIL. (09.08.2021). *Recommendation 7: Check the age of the child and parental consent while respecting the child's privacy*. https://www.cnil.fr/en/recommendation-7-check-age-child-and-parental-consent-while-respecting-childs-privacy.

[178] GCHQ, *supra* note 73 at 14.

[179] CEN, *supra* note 12 at 27.

[180] British Standards Institution, *supra* note 83 at 7-8.

[181] Family Online Safety Institute, *supra* note 156 at 6.

[182] Family Online Safety Institute. (2022). *Making Sense of Age Assurance: Enabling Safer Online Experiences*. Pg. 23. https://www.fosi.org/policy-research/making-sense-of-age-assurance-enabling-safer-online-experiences.

assurance systems, such as zero-knowledge proof or decentralisation of data collection and processing, could be appropriate in this regard.

Challenge #2: Most age assurance methods are not fully accurate

The various methods of age assurance have varying levels of accuracy, but none of them are totally accurate.[183] This is because, for example, children can use strategies to circumvent age assurance systems.[184] Even methods with the highest level of accuracy, such as hard identifiers, could be bypassed by using fake identification[185] or an adult's identification (with or without that adult's knowledge). An exception may be third-party solutions that check age against a trustworthy database (e.g., citizen registrations).

Potential solutions

There have been initiatives to quantify the accuracy of age assurance systems. For instance, in the report prepared by Age Check Certification Scheme (ACCS) for the ICO, the contours for how to measure the accuracy of age assurance systems is analysed, and metrics for demonstrating accuracy are proposed.[186] While efforts in this direction will progress going forward and should be paid due consideration, companies should generally endeavour to ascertain the accuracy of their age assurance methods and ways to improve them, and should maintain records relating to accuracy. Further, in certain situations, using a combination of age assurance methods can improve the accuracy of the age assurance implemented.

5.5. Functionality and ease of use

It is imperative that age assurance technologies are easy to use in order to further their adoption and avoid unnecessary burdens on the users.[187] Perhaps the popularity of facial age estimation technologies can be attributed to the ease of using them.[188] Further, the age assurance technologies employed must offer functionality which is appropriate to the capacity and age of the child using such technologies,[189] in line with the evolving capacities of the child principle as enshrined in Article 5 UNCRC. In this regard, albeit in the context of the AADC,

[183] Brennen, *supra* note 159 at 6.

[184] euCONSENT, *supra* note 166 at 3.

[185] Brennen, *supra* note 159 at 6-7.

[186] ACCS. (2022). *Measurement of Age Assurance Technologies*. https://ico.org.uk/media/about-the-ico/documents/4021822/measurement-of-age-assurance-technologies.pdf.

[187] 5Rights Foundation, *supra* note 21 at 49.

[188] euCONSENT, *supra* note 113 at 49.

[189] CEN, *supra* note 12 at 27.

the ICO provides five different age ranges of children to guide the service providers (0-5; 6-9; 10-12; 13-15 and 16-17).[190]

Challenge #1: Functionality could dilute effectiveness

Ensuring functionality and a smooth user experience might run counter to the effectiveness of an age assurance solution. For instance, the use of age estimation methods such as facial age estimation, which requires lesser user effort, might not provide a high level of assurance as compared to hard identifiers, which require more user effort.

Potential solutions

Again, this is an aspect to be cognisant of so that the principles of necessity and proportionality can be appropriately applied. Leveraging technology to employ age assurance in an easy manner, while not compromising on the other requirements mentioned in this section, should be the goal of age assurance providers.

Challenge #2: Diverse nature of the online world

Functionality might be hindered on account of the different age assurance methods employed by various platforms on a frequent basis, requiring users to constantly perform a multitude of actions to prove their age.

Potential solutions

Achieving interoperability among age assurance solutions by allowing users to use the same age assurance tool across platforms could help tackle this issue.[191] Efforts in this direction have already been spearheaded by initiatives such as the euCONSENT project.[192]

5.6. Inclusivity and non-discrimination

Non-discrimination, as enshrined in Article 2 UNCRC, is one of the four general principles of the UNCRC and requires that effective access to the digital environment be provided to children and that digital exclusion of children be overcome.[193] Children who have disabilities, such as intellectual and audiovisual disabilities, face difficulties in accessing the online environment, for

[190] ICO, *supra* note 66 at 32-33.

[191] Brennen, *supra* note 159 at 8.

[192] euCONSENT, (n.d.). *EUCONSENT. ELECTRONIC IDENTIFICATION AND TRUST SERVICES FOR CHILDREN IN EUROPE. Creating a safer digital world for children throughout the European Union*. https://euCONSENT.eu/.

[193] Committee on the Rights of the Child, *supra* note 4 at 2.

example, because of content being in non-accessible formats.[194] When it comes to age assurance as well, the differences in children regarding languages, abilities, socioeconomic statuses and so on, ought to be paid due consideration and sufficient flexibility is required for the age assurance methods implemented.[195] Thus, age assurance solutions must be "*accessible and inclusive to users, particularly also to users with protected characteristics*".[196] For instance, inclusive techniques to account for those with learning disabilities or cognitive impairments have been proposed in the context of website design, which can be considered for age assurance systems as well.[197]

Challenge: The various possibilities for discrimination due to age assurance

Age assurance could lead to discrimination and potential exclusion in many ways, including the following:

(a) when age verification methods that require hard identifiers, credit cards, and similar are implemented, groups such as (migrant or refugee) children or socio-economically disadvantaged people who do not have access to such documents will be prevented from using the platform.[198]

(b) Age estimation methods that use AI could suffer from algorithmic biases on the basis of age, gender, ethnicity, medical conditions, etc.[199]

(c) Users require a certain level of digital skills to navigate age assurance methods.[200] This could lead to the potential exclusion of certain users who may not be that proficient with using technology.

Potential solutions

At the outset, being mindful of the potential discriminatory effects of age assurance is of utmost importance. Conducting a child rights impact assessment (CRIA) while being cognisant of the possible exclusionary effects of age assurance could be helpful in tackling this challenge. Other measures may also be relevant in specific scenarios. For instance, if AI

[194] *Ibid* at 15.

[195] 5Rights Foundation, *supra* note 21 at 51.

[196] CEN, *supra* note 12 at 27.

[197] Karreman, J., Van der Geest, T., & Buursink, E. (2007). Accessible website content guidelines for users with intellectual disabilities. *Journal of applied research in intellectual disabilities*, *20*(6), 510-518; HeX Productions. (20.06.2022). *Making your website accessible for people with learning disabilities and cognitive impairments*. https://www.horlix.com/how-to-make-your-website-accessible-to-those-with-learning-disabilities-and-difficulties/#how-to-make-your-website-accessible-to-those-with-learning-disabilities-and-difficulties; For Web Content Accessibility Guidelines Framework, see World Wide Web Consortium. (n.d.). WCAG 2 Overview. https://www.w3.org/WAI/standards-guidelines/wcag/#versions.

[198] ICO, *supra* note 15 at 15.

[199] *Id.*

[200] European Parliamentary Research Service, *supra* note 16 at 2.

systems are used, then high-quality and relevant input data should be used to train the AI so as to minimise algorithmic biases,[201] and there should be transparency regarding how such systems are trained and deployed. Further, methods such as facial age estimation (section 4.1.7) and behavioural profiling (section 4.1.8) that use AI, could have to adhere to the requirements fastened by the proposed AI Act[202] in the future, which could assuage some of these concerns relating to discrimination.

5.7. Furthering participation and access

The requirement for a digital service provider to implement age verification solutions should support age-appropriate access to goods and services, should not amount to blocking children from accessing services they rightfully have access to, and should not result in providing children with an inferior quality of online services.[203] Age assurance should not be solely aimed at protecting children from harm and should also further their participatory rights, for instance by supporting age-appropriate design.[204] The UNCRC contains several participatory rights for children; age assurance should not hinder but instead further such rights. Providing children access to platforms is of vital importance *inter alia* because the right to participate in contemporary issues is drastically enhanced through tools such as social media.[205]

Challenge: Age assurance and its negative perceptions

Age assurance is often seen as a restrictive measure, particularly by children.[206] Such views among stakeholders could result in sufficient attention not being given to how age assurance relates to the participatory rights of children.

Potential solutions

On the one hand, age assurance should not be employed lightly, given the impact it can have on the participatory rights of children. This is why it is particularly important to consult children before enacting restrictive measures

[201] ICO, *supra* note 15 at 31.

[202] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS, COM/2021/206 final, (21.04.2021).

[203] DPC, *supra* note 16 at 45.

[204] 5Rights Foundation, *supra* note 21 at 49.

[205] Assim, U. M. (2019). Civil Rights and Freedoms of the Child. In U. Kilkelly & T. Liefaard (Eds.), *International Human Rights of Children* (p. 389–417). Springer. Pg. 398. https://doi.org/10.1007/978-981-10-4184-6_7.

[206] Family Online Safety Institute, *supra* note 182 at 11.

such as age gating,[207] and to have a sound reasoning behind why children of certain ages are prevented access from a platform (or parts of it).[208]

On the other hand, age assurance should also be viewed from the prism of increasing the participation of children in online communities. Participation can be increased *inter alia* by using age assurance solutions to determine how many of the users visiting a platform are children so that appropriate avenues can be provided in the design of the platform to further access, participation, and civic engagement by children. Raising awareness about such possibilities could also help stakeholders in developing age assurance technologies not merely as a restrictive measure but as an empowering tool.

5.8. Transparency and accountability

Users must be provided with adequate and intelligible information by companies regarding the age assurance method employed and how it operates.[209] This is an important requirement from various perspectives, such as data protection. Additionally, platforms must be demonstrably accountable for the implementation of age assurance in compliance with applicable law, and in adherence to the requirements mentioned in this section.[210]

Challenge: Making age assurance methods intelligible to children

The added difficulty when it comes to protecting children online is that platforms should present information relating to age assurance in a manner that is attractive, understandable and recognisable given the age of the child who is accessing their service.[211] This may prove challenging given the different ages of children who access a platform and their varying mental capacities.

Potential solutions

Co-opting the guidance on informed consent and transparency under the GDPR, by use of just-in-time notices, layered notices, standardised icons etc.,[212] for explaining the working of age assurance systems could be helpful in this regard. Particularly, adding formats that may be attractive to children, such as chatbots, videos, games, or comics may be helpful in getting the

[207] van der Hof, *supra* note 24 at 9.

[208] UNICEF, *supra* note 77 at 54.

[209] CEN, *supra* note 12 at 27; British Standards Institution, *supra* note 83 at 12.

[210] 5Rights Foundation, *supra* note 21 at 51.

[211] ACCS. (2021). *Technical Requirements for Age Appropriate Design for Information Society Services*. Pg. 29. https://ico.org.uk/media/for-organisations/documents/2620427/accs-3-2021-technical-requirements-aadc.pdf.

[212] Article 29 Working Party. (11.04.2018). *Guidelines on transparency under Regulation 2016/679*. WP 260. https://ec.europa.eu/newsroom/article29/items/622227.

information across.[213] Further, increasing the participation of children and taking their views relating to age assurance methods can provide valuable inputs on how to explain the functioning of age assurance to children.

5.9. Notification, challenge, and redressal mechanisms

Closely related to the transparency and accountability requirement is the need to follow due process regarding age assurance decisions. In the event that age assurance technologies incorrectly determine the age of the users, users should have recourse against such determination.[214] This should be enabled by having an easy and expedient mechanism to challenge age assurance decisions and take redressal against the same.[215] Even if the user merely wants to notify platforms that an incorrect decision was taken, there must be an avenue for that. This is important for procedural fairness as much as providing an avenue for age assurance providers to obtain feedback regarding the accuracy of their technologies.

Challenge: Lack of regulation and standards

Equally relevant to other requirements as well, the lack of concrete regulation focused on age assurance, and standards at the EU and international level, presents a hindrance in ensuring that platforms employ such due process measures, including the provision of challenge and redressal mechanisms.

Potential solutions

Regulators such as the CNIL, AEPD, CNMC and KJM have undertaken various initiatives relating to age assurance which can contribute to the body of knowledge regarding a fair implementation of age assurance. Regulators such as the ICO and Ofcom in the UK may also provide guidance on how to make age assurance providers act in a fair manner with the users, when such regulators enforce instruments such as the AADC and the UK Online Safety Act 2023.

Further, organisations such as the ISO and the Institute of Electrical and Electronics Engineers (IEEE) intend to issue standards focused on age assurance systems in the near future[216]. In addition to aspects pertaining to

[213] See on child-friendly transparency, Milkaite, I., & Lievens, E. (2020). Child-friendly transparency of data processing in the EU: from legal requirements to platform policies. *Journal of Children and Media*, *14*(1), 5-21. Pg. 16-17.

[214] Brennen, *supra* note 159 at 8.

[215] 5Rights Foundation, *supra* note 21 at 50.

[216] ISO, *supra* note 138; IEEE. (n.d.). P2089.1 *Standard for Online Age Verification*. https://standards.ieee.org/ieee/2089.1/10700/#:~:text=Standard%20for%20Online%20Age%20Verification&text=This%20standard%20establishes%20a%20framework,the%20age%20assurance%20process%2C%202.

the processes to be followed by platforms, these standards could give more insight into issues such as the level of age assurance required for the protection of children, to be implemented by specific platforms. Furthermore, these standards should include consideration of the effects of age assurance on the digital ecosystem and, more specifically, on the effective enforcement of legislation, in order to ensure both adequate protection of, and age-appropriate design for, children, as well as the creation of a level playing field for companies.

Additionally, it would be welcome if online platforms can be provided with guidance on how to ensure a high level of privacy, security and safety for children, while respecting their fundamental freedoms, which could include guidance on the consistent application of age assurance. Article 28(4) DSA empowers the European Commission to issue such guidelines. It is also worth noting that the European Commission has recently formed a task force, with Member States, to promote cooperation and identify best practices relating to age verification[217].

Meanwhile, platforms should have clearly laid down policies and procedures regarding such notification, challenge and redressal avenues, and communicate the same to users in an intelligible and transparent manner.

5.10. Hearing the views of children

Children have a right to be heard under Article 12 UNCRC which is one of its four general principles, and digital service providers should appropriately engage with children and pay due heed to their views.[218] Fostering the active participation of children in decision-making for the digital environment is also a key pillar of the BIK+ strategy.[219] With respect to age assurance, age assurance providers should empower children in exercising this right by affording them opportunities to convey their views on aspects such as privacy, functionality and ease of use, transparency and accountability etc. of age assurance systems. For instance, in determining functionality and ease of use, it may be necessary to conduct tests with users, including children, and this would require involving children (and potentially their parents or caretakers). Such opportunities could be provided within the framework of conducting a CRIA (when there is a CRIA) and even otherwise.

[217] European Commission. (30.01.2024). *Digital Services Act: Task Force on Age Verification*. https://digital-strategy.ec.europa.eu/en/news/digital-services-act-task-force-age-verification-0.

[218] Committee on the Rights of the Child, *supra* note 4 at 3.

[219] European Commission, *supra* note 7 at 9.

Challenge: Lack of expertise and tokenism

Age assurance providers may not have the requisite expertise and know-how in collaborating with children, which can be a more acute challenge for smaller companies with limited resources. Even where such capabilities exist, listening to the views of children could be undertaken by some companies as a form of tokenism, which could amount to youth-washing.[220]

Potential solutions

Age assurance providers can engage with policy bodies that work with children, parents and schools, to gain insights into the views of children. There are also secondary sources and studies that are present[221] (and still being undertaken) that can be investigated for inputs. Leveraging technology for soliciting children's (and potentially their parents) views through online surveys, social media polls etc., and conducting co-creational workshops, could also be useful to this end.

[220] Youth-washing is when it is superficially made to seem as if young people are being heard, without actually paying heed to their views. See The Scotsman. (04.11.2021). *'COP 26 is a youth-washing project', according to young activists participating in the conference*. https://www.scotsman.com/news/environment/cop-26-is-a-youth-washing-project-say-young-activists-3445764.

[221] E.g., Family Online Safety Institute, *supra* note 156 at 11; euCONSENT, *supra* note 113 at 49.

6. Conclusion

It is estimated that one-third of internet users in the world are children.[222] The internet provides a lot of opportunities for children to access knowledge, to communicate, to upskill themselves, and so on.[223] However, children also face several risks and harms online to their rights, well-being and development. This is why lawmakers enact instruments for the protection of children online, including instruments which mandate age assurance (or, more specifically, age verification), and those which may require age assurance to be employed as a duty of care.

However, as can be seen from this report, age assurance is a complex topic, and it is far from straightforward as to how age assurance is to be implemented in given situations. The various methods of age assurance have their own advantages and disadvantages. Further, even among the requirements that age assurance should have, there are contrasting principles, and a balance needs to be struck between the various requirements that are sought to be met.

Additionally, one has to be aware of the fact that there are competing stakeholder interests when it comes to age assurance. For instance, age assurance could be viewed by regulators and parents as necessary to protect children, while children could view it as a restriction on their right to internet usage.[224] Further, even if implemented for the (online) protection of the rights and well-being of children, age assurance would have an effect on all other users as well, whose user experience and privacy could be negatively affected due to age assurance measures.[225] This is why it is often stated that age assurance should not be construed as a silver bullet for online child protection.[226] Age assurance is only one of the many tools to protect[227] and further the experiences of children online.[228]

However, this does not mean that age assurance should not be considered as a viable option since it can also still be a very useful tool in protecting children

---

[222] GCHQ, *supra* note 73 at 1; Livingstone, S., Carr, J., & Byrne, J. (Jan 2016). One in three: Internet governance and children's rights. *UNICEF*. Pg. 7. https://www.unicef-irc.org/publications/pdf/idp_2016_01.pdf.

[223] British Standards Institution, *supra* note 83 at ix.

[224] Family Online Safety Institute, *supra* note 182 at 11.

[225] EFF, *supra* note 164.

[226] 5Rights Foundation, *supra* note 21 at 7.

[227] Center for Information Policy Leadership. (16.03.2023). *Age Assurance and Age Verification Tools: Takeaways from CIPL Roundtable*. https://www.informationpolicycentre.com/cipl-blog/age-assurance-and-age-verification-tools-takeaways-from-cipl-roundtable.

[228] euCONSENT, *supra* note 166 at 7.

online. Especially with the development of technology and a more proactive approach from standardisation bodies and policymakers, a robust and context-specific age assurance regime for the internet can be a reality. More privacy-friendly options may become available (more widely) over time. In the future, efforts by standardisation bodies such as the ISO and IEEE, work by regulators such as the CNIL, AEPD, CNMC, KJM, ICO and Ofcom, as well as guidance from the European Commission through, among others, the proposed European standard for online age verification and code of conduct on age-appropriate design, could provide clear guidelines on how to implement age assurance solutions in an appropriate manner.

Bibliography

- 5Rights Foundation. (Oct 2020). *Building the Digital World that Young People Deserve. Priorities for the Online Harms Bill*. https://5rightsfoundation.com/uploads/5rights-priorities---online-harms-bill.pdf.
- 5Rights Foundation. (Oct 2021). *But how do they know it is a child? Age Assurance in the Digital World*. https://5rightsfoundation.com/uploads/But_How_Do_They_Know_It_is_a_Child.pdf.
- Age Check Certification Scheme. (2021). *Technical Requirements for Age Appropriate Design for Information Society Services*. https://ico.org.uk/media/for-organisations/documents/2620427/accs-3-2021-technical-requirements-aadc.pdf.
- Age Check Certification Scheme. (2022). *Measurement of Age Assurance Technologies*. https://ico.org.uk/media/about-the-ico/documents/4021822/measurement-of-age-assurance-technologies.pdf.
- Article 29 Working Party. (11.04.2018). *Guidelines on transparency under Regulation 2016/679*. WP 260. https://ec.europa.eu/newsroom/article29/items/622227.
- Article 29 Working Party. (27.02.2013). *Opinion 02/2013 on apps on smart devices*. WP 202. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf.
- Assim, U. M. (2019). Civil Rights and Freedoms of the Child. In U. Kilkelly & T. Liefaard (Eds.), *International Human Rights of Children* (p. 389–417). Springer. https://doi.org/10.1007/978-981-10-4184-6_7.
- Bodle, R. (2013). The ethics of online anonymity or Zuckerberg vs. "Moot". *Acm Sigcas Computers and Society*, *43*(1), 22-35. https://dl.acm.org/doi/10.1145/2505414.2505417.
- Brennen, S., & Perault, M. (2023). Keeping Kids Safe Online: How Should Policymakers Approach Age Verification? *The Center for Growth and Opportunity*. https://www.thecgo.org/research/keeping-kids-safe-online-how-should-policymakers-approach-age-verification/.
- British Standards Institution. (31.03.2018). *PAS 1296:2018 Online age checking. Provision and use of online age check services. Code of Practice*.
- Center for Information Policy Leadership. (16.03.2023). *Age Assurance and Age Verification Tools: Takeaways from CIPL Roundtable*.

https://www.informationpolicycentre.com/cipl-blog/age-assurance-and-age-verification-tools-takeaways-from-cipl-roundtable.

- Cerulli-Harms, A., Münsch, M., Thorun, C., Michaelsen, F., & Hausemer, P. (2020). Loot boxes in online games and their effect on consumers, in particular young consumers. *Publication for the Committee on the Internal Market and Consumer Protection (IMCO), Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg*, *202*. https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652727/IPOL_STU(2020)652727_EN.pdf.
- CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION, OJ C 326, 26.10.2012, p. 391–407.
- Commission for the Protection of Minors in the Media. (n.d.). *Supervision*. https://www.kjm-online.de/en/supervision.
- Commission for the Protection of Minors in the Media. (12.05.2022). Kriterien zur Bewertung von Konzepten für Altersverifikationssysteme als Elemente zur Sicherstellung geschlossener Benutzergruppen in Telemedien nach § 4 Abs. 2 S. 2 JMStV. https://www.kjm-online.de/fileadmin/user_upload/KJM/Aufsicht/Technischer_Jugendmedienschutz/AVS-Raster_ueberarbeitet_gueltig_seit_12.05.2022__004_.pdf.
- Commission for the Protection of Minors in the Media. (24.05.2022). *KJM bewertet Altersverifikationssysteme mit biometrischer Alterskontrolle positiv*. https://www.kjm-online.de/service/pressemitteilungen/meldung/kjm-bewertet-altersverifikationssysteme-mit-biometrischer-alterskontrolle-positiv.
- Commission Nationale Informatique & Libertés. (09.08.2021). *Recommendation 7: Check the age of the child and parental consent while respecting the child's privacy*. https://www.cnil.fr/en/recommendation-7-check-age-child-and-parental-consent-while-respecting-childs-privacy.
- Commission Nationale Informatique & Libertés. (22.09.2022). *Online age verification: balancing privacy and the protection of minors*. https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors.
- Commission Nationale Informatique & Libertés. (21.02.2023). *Contrôle de l'âge pour l'accès aux sites pornographiques*. https://www.cnil.fr/fr/controle-de-lage-pour-lacces-aux-sites-pornographiques.
- Committee for Standardization and European Committee for Electrotechnical Standardization. (Sep 2023). *Age appropriate digital*

services framework. https://www.cencenelec.eu/media/CEN-CENELEC/CWAs/ICT/cwa18016_2023.pdf.

- Committee on the Rights of the Child. (Nov 2003). *General Comment No. 5 (2003) General Measures of Implementation of the Convention on the Rights of the Child (Arts. 4, 42 and 44, Para. 6)*. CRC/GC/2003/527. https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsiQql8gX5Zxh0cQqSRzx6Zd2%2FQRsDnCTcaruSeZhPr2vUevjbn6t6GSi1fheVp%2Bj5HTLU2Ub%2FPZZtQWn0jExFVnWuhiBbqgAj0dWBoFGbK0c.
- Committee on the Rights of the Child. (02.03.2021). *General comment No. 25 (2021) on children's rights in relation to the digital environment*. CRC/C/GC/25. https://digitallibrary.un.org/record/3906061?ln=en.
- Congressional Research Service. (23.03.2023). *Challenges with Identifying Minors Online*. https://crsreports.congress.gov/product/pdf/IN/IN12055#:~:text=Potential%20Challenges%20with%20Identifying%20Minors,as%20those%20younger%20than%2013.
- Congressional Research Service. (17.08.2023). *Online Age Verification (Part I): Current Context*. https://crsreports.congress.gov/product/pdf/LSB/LSB11020.
- Congressional Research Service. (17.08.2023). *Online Age Verification (Part II): Constitutional Background*. https://crsreports.congress.gov/product/pdf/LSB/LSB11021.
- Data Protection Commissioner. (Dec 2021). *Fundamentals for a Child-Oriented Approach to Data Processing*. https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf.
- Devi, S., Kotian, S., Kumavat, M., & Patel, D. (2022). Digital Identity Management System Using Blockchain. *Available at SSRN 4127356*.
- Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council, OJ L 149, 11.6.2005, p. 22–39.
- 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, OJ L 303, 28.11.2018, p. 69–92.

- Eekelaar, J. & and Tobin, J. (2019). Art. 3 the Best Interests of the Child. In Tobin, J. (Ed.), *The UN Convention on the Rights of the Child: A Commentary* (p. 99). Oxford: Oxford University Press.
- Electronic Frontiers Foundation. (05.09.2023). *UK Online Safety Bill Will Mandate Dangerous Age Verification for Much of the Web*. https://www.eff.org/deeplinks/2023/09/uk-online-safety-bill-will-mandate-dangerous-age-verification-much-web.
- Electronic Frontiers Foundation. (10.03.2023). *Age Verification Mandates Would Undermine Anonymity Online*. https://www.eff.org/deeplinks/2023/03/age-verification-mandates-would-undermine-anonymity-online.
- eSafety Commissioner, Australia. (Mar 2023). *Roadmap for age verification and complementary measures to prevent and mitigate harms to children from online pornography*. https://www.esafety.gov.au/sites/default/files/2023-08/Roadmap-for-age-verification_2.pdf.
- eSafety Commissioner, Australia. (Aug 2023). *Roadmap for age verification and complementary measures to prevent and mitigate harms to children from online pornography*. https://www.esafety.gov.au/sites/default/files/2023-08/Age-verification-background-report.pdf.
- euCONSENT, (n.d.). *EUCONSENT. ELECTRONIC IDENTIFICATION AND TRUST SERVICES FOR CHILDREN IN EUROPE. Creating a safer digital world for children throughout the European Union*. https://euCONSENT.eu/.
- euCONSENT. (29.06.2021). *D5.1 Common Vocabulary*. https://euCONSENT.eu/project-deliverables/.
- euCONSENT. (Sept 2021). *EU Member State Legal Framework*. https://euCONSENT.eu/project-deliverables/.
- euCONSENT. (Sept 2021). *Understanding of user needs and problems: A rapid evidence review of age assurance and parental controls*. https://euCONSENT.eu/project-deliverables/.
- euCONSENT. (02.01.2022). *D2.2 EU Methods for AVMSD and GDPR Compliance Report*. https://euCONSENT.eu/project-deliverables/.
- euCONSENT. (08.05.2022). *D6.3.3 Pilot Execution Report*. https://euCONSENT.eu/project-deliverables/.
- European Commission. (11.05.2022). *A Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+)*.

https://digital-strategy.ec.europa.eu/en/library/digital-decade-children-and-youth-new-european-strategy-better-internet-kids-bik.

- European Commission. (11.05.2022). *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. A Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+)*. COM(2022) 212 final. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022DC0212.
- European Commission. (30.01.2024). *Digital Services Act: Task Force on Age Verification*. https://digital-strategy.ec.europa.eu/en/news/digital-services-act-task-force-age-verification-0.
- European Data Protection Supervisor. (n.d.). *Necessity & Proportionality*. https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en.
- European Parliamentary Research Service. (Feb 2023). *Online age verification methods for children*. https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/739350/EPRS_ATA(2023)739350_EN.pdf.
- European Union Agency for Cybersecurity. (Oct 2021). *ENISA THREAT LANDSCAPE 2021*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021?v2=1.
- European Union Agency for Fundamental Rights, (n.d.). *Age of majority*. https://fra.europa.eu/en/publication/2017/mapping-minimum-age-requirements/age-majority#:~:text=The%20age%20of%20majority%20is%2018%20years%20in%20all%20EU,child%20gains%20full%20legal%20capacity.
- Family Online Safety Institute. (2022). *Making Sense of Age Assurance: Enabling Safer Online Experiences*. https://www.fosi.org/policy-research/making-sense-of-age-assurance-enabling-safer-online-experiences.
- Family Online Safety Institute. (July 2023). *Coming to Terms with Age Assurance*. https://www.fosi.org/policy-research/coming-to-terms-with-age-assurance.
- Finance Magnates. (13.03.2023). *Identity on the Blockchain: Building a More Secure Future*. https://www.financemagnates.com/cryptocurrency/education-centre/identity-on-the-blockchain-building-a-more-secure-future/.
- French Law no. 2023-566, (07.07.2023).

- Government Communications Headquarters UK. (Nov 2020). *VoCO (Verification of Children Online). Phase 2 Report*. https://www.gov.uk/government/publications/voco-verification-of-children-online-phase-2-report.
- HeX Productions. (20.06.2022). *Making your website accessible for people with learning disabilities and cognitive impairments*. https://www.horlix.com/how-to-make-your-website-accessible-to-those-with-learning-disabilities-and-difficulties/#how-to-make-your-website-accessible-to-those-with-learning-disabilities-and-difficulties.
- Hogan Lovells. (02.01.2024). *Spanish Data Protection Agency's Guidance on age verification*. https://www.engage.hoganlovells.com/knowledgeservices/viewContent.action?key=Ec8teaJ9Vap8ahmeIu1HI17eOOGbnAEFKCLORG72fHz0%2BNbpi2jDfaB8lgiEyY1JAvAvaah9lF3dzoxprWhI6w%3D%3D&nav=FRbANEucS95NMLRN47z%2BeeOgEFCt8EGQ0qFfoEM4UR4%3D&emailtofriendview=true&freeviewlink=true.
- Information Commissioner's Office. (14.10.2021). *Information Commissioner's opinion: Age Assurance for the Children's Code*. https://ico.org.uk/media/about-the-ico/documents/4018659/age-assurance-opinion-202110.pdf.
- Information Commissioner's Office. (April 2022). *Regulatory Sandbox Final Report: Yoti*. https://ico.org.uk/media/for-organisations/documents/4020427/yoti-sandbox-exit_report_20220522.pdf.
- Information Commissioner's Office. (17.10.2022). *Age appropriate design: a code of practice for online services*. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/.
- Information Commissioner's Office. (n.d.). *'Likely to be accessed' by children – FAQs, list of factors and case studies.* https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/likely-to-be-accessed-by-children/#threshold.
- Information Commissioner's Office. (n.d.). *The ICO's response to the Call for Evidence and roundtables on age assurance*. https://ico.org.uk/media/about-the-ico/consultations/4023900/20230203-response-to-aa-cfe-and-roundtables-v1_1.pdf.
- Institute of Electrical and Electronics Engineers. (n.d.). *P2089.1 Standard for Online Age Verification*. https://standards.ieee.org/ieee/2089.1/10700/#:~:text=Standard%20for%

20Online%20Age%20Verification&text=This%20standard%20establishes%20a%20framework,the%20age%20assurance%20process%2C%202.

- International Organization for Standardization and International Electrotechnical Commission. (2013). *Information technology — Security techniques — Information security management systems — Requirements*. ISO/IEC 27001:2013(E).
- International Organization for Standardization and International Electrotechnical Commission. (2013). *Information technology — Security techniques — Code of practice for information security controls*. ISO/IEC 27002:2013(E).
- International Organization for Standardization. (Nov 2021). *ISO Working Draft Age Assurance Systems Standard*. https://euCONSENT.eu/download/iso-working-draft-age-assurance-systems-standard/.
- Karreman, J., Van der Geest, T., & Buursink, E. (2007). Accessible website content guidelines for users with intellectual disabilities. *Journal of applied research in intellectual disabilities*, *20*(6), 510-518.
- Le Monde. (29.06.2023). *France requires parental consent for under-15s on social media*. https://www.lemonde.fr/en/france/article/2023/06/29/france-requires-parental-consent-for-under-15s-on-social-media_6039514_7.html.
- Lievens, E. (2021). Growing up with digital technologies: how the precautionary principle might contribute to addressing potential serious harm to children's rights. *Nordic Journal of Human Rights*, *39*(2), 128-145.
- Livingstone, S. (2013). Online risk, harm and vulnerability: Reflections on the evidence base for child Internet safety policy. *ZER: Journal of Communication Studies*, *18*(35), 13-28. https://www.researchgate.net/publication/285900088_Online_risk_harm_and_vulnerability_Reflections_on_the_evidence_base_for_child_internet_safety_policy.
- Livingstone, S., Carr, J., & Byrne, J. (Jan 2016). One in three: Internet governance and children's rights. *UNICEF*. https://www.unicef-irc.org/publications/pdf/idp_2016_01.pdf.
- Livingstone, S., & Stoilova, M. (2021). The 4Cs: Classifying online risk to children. *Leibniz-Institut Für Medienforschung | Hans-Bredow-Institut (HBI)*. https://doi.org/10.21241/ssoar.71817.
- Milkaite, I., & Lievens, E. (2020). Child-friendly transparency of data processing in the EU: from legal requirements to platform policies. *Journal of Children and Media*, *14*(1), 5-21.

- National Institute of Standards and Technology. (n.d.). *Face Analysis Technology Evaluation (FATE) Age Estimation & Verification*. https://pages.nist.gov/frvt/html/frvt_age_estimation.html.
- National Institute of Standards and Technology. (20.09.2023). *What's Wrong With This Picture? NIST Face Analysis Program Helps to Find Answers*. https://www.nist.gov/news-events/news/2023/09/whats-wrong-picture-nist-face-analysis-program-helps-find-answers.
- National Markets and Competition Commission. (n.d.). *PUBLIC CONSULTATION ON THE CRITERIA FOR ENSURING THE APPROPRIATENESS OF AGE VERIFICATION SYSTEMS ON VIDEO-SHARING PLATFORM SERVICES FOR CONTENT THAT IS HARMFUL FOR MINORS*. INF/DTSA/329/23. https://www.cnmc.es/sites/default/files/editor_contenidos/Audiovisual/1_1_INF_DTSA_329_23_Public consultation age verification CNMC Spain_eng.pdf
- *NetChoice LLC, v. Rob Bonta*, Case No. 22-cv-08861-BLF, United States District Court, Northern District of California, San Jose Division.
- Nomos. (02.10.2023). *The introduction of a digital age of majority and new obligations for social networks*. https://www.lexology.com/library/detail.aspx?g=c8be7729-5509-40e9-8365-0eb7ebdd3d35.
- Office of Communications. (05.12.2023). *Guidance on age assurance and other Part 5 duties for service providers publishing pornographic content on online services*. https://www.ofcom.org.uk/__data/assets/pdf_file/0018/272601/guidance-part-5-annexe-2.pdf.
- Online Safety Act (2023). https://www.legislation.gov.uk/ukpga/2023/50/contents/enacted.
- Organization for Economic Cooperation and Development. (2021). *Children in the digital environment: Revised typology of risks*. https://www.oecd-ilibrary.org/science-and-technology/children-in-the-digital-environment_9b8f222e-en.
- Paik, S., Mays, K. K., & Katz, J. E. (2022). Invasive Yet Inevitable? Privacy Normalization Trends in Biometric Technology. *Social Media+ Society*, *8*(4), 20563051221129147.
- Pan European Game Information. (n.d.). *PEGI age ratings*. https://pegi.info/page/pegi-age-ratings.
- PricewaterhouseCoopers. (2019). *Blockchain and Digital Identity: the path to Self Sovereign Identity*. https://www.pwc.com/it/it/publications/assets/docs/blockchain-and-digital-identity.pdf.

- Privacy by Design Foundation. (n.d.). *About IRMA*. https://privacybydesign.foundation/irma-en/.
- Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, COM/2021/281 final, (03.06.2021).
- Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS, COM/2021/206 final, (21.04.2021).
- Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM(2022) 454 final, (15.09.2022).
- 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, OJ L 119, 4.5.2016, p. 1–88.
- 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, OJ L 277, 27.10.2022, p. 1–102.
- Reuters. (14.12.2023). *Spain readies age-checking tech to protect children from adult online content*. https://www.reuters.com/world/europe/spain-readies-age-checking-tech-protect-children-adult-online-content-2023-12-14/.
- Richards, N. (2015). *Intellectual privacy: Rethinking civil liberties in the digital age*. Oxford University Press, USA.
- Spanish Data Protection Authority. (Dec 2023). *Decálogo de principios. Verificación de edad y protección de personas menores de edad ante contenidos inadecuados.* https://www.aepd.es/guias/decalogo-principios-verificacion-edad-proteccion-menores.pdf.
- TechTarget. (n.d.). *facial recognition*. https://www.techtarget.com/searchenterpriseai/definition/facial-recognition.
- Theobald, M. (2019). UN Convention on the Rights of the Child: “Where are we at in recognising children’s rights in early childhood, three decades on…?”. *International Journal of Early Childhood*, *51*(3), 251-257. https://doi.org/10.1007/s13158-019-00258-z.

- The Scotsman. (04.11.2021). *'COP 26 is a youth-washing project', according to young activists participating in the conference*. https://www.scotsman.com/news/environment/cop-26-is-a-youth-washing-project-say-young-activists-3445764.
- The Verge. (18.09.2023). *Court blocks California's online child safety law*. https://www.theverge.com/2023/9/18/23879489/california-age-appropriate-design-code-act-blocked-unconstitutional-first-amendment-injunction.
- Tisdall, E. K. M., & Cuevas-Parra, P. (2022). Beyond the familiar challenges for children and young people's participation rights: The potential of activism. *The International Journal of Human Rights*, *26*(5), 792-810.
- United Nations Children's Fund. (Apr 2021). *Digital Age Assurance Tools and Children's Rights Online across the Globe: A Discussion Paper*. https://c-fam.org/wp-content/uploads/Digital-Age-Assurance-Tools-and-Childrens-Rights-Online-across-the-Globe.pdf.
- United States Federal Reserve System. (May 2023). *Economic Well-Being of U.S. Households in 2022*. https://www.federalreserve.gov/publications/files/2022-report-economic-well-being-us-households-202305.pdf.
- van der Hof, S., Lievens, E., Milkaite, I., Verdoodt, V., Hannema, T., & Liefaard, T. (2020). The child's right to protection against economic exploitation in the digital world. *The International Journal of Children's Rights*, *28*(4), 833-859. https://brill.com/view/journals/chil/28/4/article-p833_833.xml?language=en.
- van der Hof, S., & Ouburg, S. (2021). Methods for Obtaining Parental Consent and Maintaining Children Rights, WP2: Existing Methods, User Needs and Requirements. Deliverable D2.3 euCONSENT. *Leiden University*.
- van der Hof, S., & Ouburg, S. (2022). 'We Take Your Word for It'-A Review of Methods of Age Verification and Parental Consent in Digital Services. *Eur. Data Prot. L. Rev.*, *8*, 61. https://edpl.lexxion.eu/article/EDPL/2022/1/10.
- van Tiel, J. (2020). *Cyberbullying, an overlooked and ever growing danger to the development of children*. Technical report, KidsRights.
- World Bank. (2019). *Identification for Development (ID4D), Practitioner's Guide*. https://id4d.worldbank.org/guide.
- World Wide Web Consortium. (n.d.). *WCAG 2 Overview*. https://www.w3.org/WAI/standards-guidelines/wcag/#versions.

.

Getting in touch with the EU

In person

All over the European Union there are hundreds of Europe Direct centres. You can find the address of the centre nearest you online (european-union.europa.eu/contact-eu/meet-us_en).

On the phone or in writing

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
- at the following standard number: +32 22999696,
- via the following form: european-union.europa.eu/contact-eu/write-us_en.

Finding information about the EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website (european-union.europa.eu).

EU publications

You can view or order EU publications at op.europa.eu/en/publications. Multiple copies of free publications can be obtained by contacting Europe Direct or your local documentation centre (european-union.europa.eu/contact-eu/meet-us_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex (eur-lex.europa.eu).

EU open data

The portal data.europa.eu provides access to open datasets from the EU institutions, bodies and agencies. These can be downloaded and reused for free, for both commercial and non-commercial purposes. The portal also provides access to a wealth of datasets from European countries.

KK-02-24-228-EN-N

Publications Office
of the European Union