EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

Opinion 36/2026

on the Proposal for a Regulation EU KIDS ACT - 'EU Keeping Internet Digital Spaces Accountable and Trustworthy'

edps.europa.eu

The European Data Protection Supervisor (EDPS) is an independent institution of the EU, responsible under Article 52(2) of Regulation 2018/1725 'With respect to the processing of personal data... for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to data protection, are respected by Union institutions and bodies', and under Article 52(3)'... for advising Union institutions and bodies and data subjects on all matters concerning the processing of personal data'.

Wojciech Rafał Wiewiórowski was appointed as Supervisor on 5 December 2019 for a term of five years. The selection procedure for a new EDPS mandate for a term of five years is still ongoing.

*Under **Article 42(1)** of Regulation 2018/1725, the Commission shall 'following the adoption of proposals for a legislative act, of recommendations or of proposals to the Council pursuant to Article 218 TFEU or when preparing delegated acts or implementing acts, consult the EDPS where there is an impact on the protection of individuals' rights and freedoms with regard to the processing of personal data'.*

This Opinion relates to the Commission Proposal for a Regulation EU KIDS ACT - 'EU Keeping Internet Digital Spaces Accountable and Trustworthy'[1]. This Opinion does not preclude any future additional comments or recommendations by the EDPS, in particular if further issues are identified or new information becomes available. Furthermore, this Opinion is without prejudice to any future action that may be taken by the EDPS in the exercise of his powers pursuant to Regulation (EU) 2018/1725. This Opinion is limited to the provisions of the Proposal that are relevant from a data protection perspective.

[1] COM(2026) 681 final.

Executive Summary

On 17 September 2026, the European Commission presented its Proposal for a Regulation on the EU KIDS ACT ('EU Keeping Internet Digital Spaces Accountable and Trustworthy').

The EDPS strongly supports the Proposal's objectives of protecting children online and preventing regulatory fragmentation in the EU single market. Several online services pose substantial risks to minors and protecting children must be a priority. Under Article 24(1) of the EU Charter of fundamental rights, children have the right to such protection and care as is necessary for their well-being. As several Member States are advancing national legislation limiting minors' access to certain online services, an EU-level response is necessary to avoid fragmentation. While recognising that the Proposal aims to address certain online services in particular, the EDPS recommends harmonising the age of consent for personal data processing in relation to all information society services in order to enhance coherence between the Proposal and the GDPR, simplify the regulatory framework and further reduce fragmentation.

The EDPS welcomes the Proposal's emphasis on 'safety by design'. Several requirements of the Proposal – for example on addictive design, recommender systems, safe settings and economic transactions – concern practices that can also be harmful, unfair or even unlawful when applied to adults, in particular when they are vulnerable. While risks stemming from the design or functioning of online services are generally higher for children than for adults, both should be appropriately protected.

The Proposal provides for several measures that interfere with the fundamental rights of children and adults, including freedom of expression, freedom of assembly, privacy and data protection. Any such interference must comply with Article 52 of the Charter. In addition to being the least intrusive among effective options, the selected measures must also be limited to what is necessary and proportionate to achieve the legitimate objective of protecting children online.

The EDPS recognises the efforts to minimise the interference with fundamental rights, including the rights to privacy and data protection. This is evident where the Proposal requires taking into account minors' privacy and developing agency and autonomy when establishing guardian-controlled access to and use of certain services, but also where it requires age assurance to ensure a high level of accuracy, reliability, security, robustness, non-intrusiveness, privacy and data protection, and non-discrimination. The EDPS very much welcomes the requirement that, in line with the EDPB Statement on Age Assurance, solutions for age assurance and verification of parental responsibility may not enable the identification of users nor be used to locate, track, target, advertise to or profile them. It is also welcomes that providers carrying out age assurance would be precluded from re-using that information for other purposes and that assurance solutions should be based on state-of-the-art privacy-enhancing technologies including zero knowledge proof.

The scope of any measure that interferes with fundamental rights must be limited to that what is necessary and proportionate. In this regard, the EDPS observes that the Proposal would affect several services that individuals (both minors and adults) use on a regular basis and does not concern services that specialise in adult content. While recognising that certain features of the services in scope of the Proposal pose enhanced risks to minors, it is important to consider the potential risks for all individuals.

Measures that interfere with fundamental rights must also be effective in pursuing their protective purpose. In this regard, the EDPS considers it of utmost importance to take into account possible risks of circumvention of age assurance mechanisms and the principle that protection should not necessarily mean exclusion. It is equally important to consider the full range of possible measures to advance the Proposal's aim, taking into account their effectiveness, degree of interference, and the best interests of the child. The EDPS invites the co-legislators to carefully consider which specific features of the services in scope of the Proposal effectively require use of age assurance as means to mitigate the risks for minors in particular and which risks could be effectively addressed by imposing safety by design measures that benefit all users, in combination with alternative measures such as additional reporting functionalities for minors, complementary tools for guardians and digital literacy initiatives.

Once that assessment has been made, the EDPS stresses the need to take into account the maturity and availability of age assurance solutions that provide a high level of privacy, such as zero knowledge proofs. Age assurance and parental verification obligations under the Proposal should only enter into application when the privacy-preserving solutions envisaged by Proposal are effectively available across the EU. Age estimation should only be allowed as an alternative where sufficient safeguards are in place to ensure they do not lower the level of privacy, safety and security of individuals.

This Opinion aims to provide constructive advice to ensure that the Proposal achieves its objective of providing a high level of privacy, security and safety for minors, while preserving a high level of protection of fundamental rights for all users of the online services in scope. The Opinion pays particular attention to different age assurance mechanisms envisaged by the Proposal, as well as the mechanisms to establish parental responsibility and tools for guardians. Specific recommendations also invite to clarify the relationship between the Proposal and existing data protection rules, in order to ensure a coherent framework that provides legal certainty to all actors involved.

Contents

1. Introduction 5

2. General remarks 6

3. Interplay with EU data protection law 9

4. Delayed creation and use of accounts for OSNs and VSPs 10

5. Tools for guardians 10

6. Verification of parental responsibility 11

7. Safety by design 13
   - 7.1. Obligations for OSNs and VSPs 14
   - 7.2. Obligations for AI companions and general conversational chatbots 15
   - 7.3. Obligations for providers of online games 16
   - 7.4. Age ratings and obligations of software application stores 16
   - 7.5. Codes of Conduct on age rating and online games 17
   - 7.6. Agency of minors and child-friendly reporting and support tools for minors 18

8. Age Assurance 18
   - 8.1. Alternative age assurance methods 20
   - 8.2. Age signals provided by providers of operating system 21
   - 8.3. Specifications and governance of the EU Age Verification Scheme 21
   - 8.4. Availability and accessibility of verification solutions 22
   - 8.5. Existing accounts 22

9. Competences, supervision and enforcement 23

10. Conclusions 24

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC ('EUDPR')[2], and in particular Article 42(1) thereof,

HAS ADOPTED THE FOLLOWING OPINION:

1. Introduction

1. On 17 September 2026, the European Commission issued the Proposal for a Regulation EU KIDS ACT - 'EU Keeping Internet Digital Spaces Accountable and Trustworthy'[3] ('the Proposal').

2. The objective of the Proposal is to fill the gap in the protection of minors in the current online environment. The Staff Working Document ('SWD') accompanying the Proposal provides an overview of the risks minors face online (e.g., cyberbullying, exposure to harmful content, privacy infringements, grooming, disinformation, radicalisation), as well as supporting evidence for each of them[4].

3. The Proposal also aims to reduce risks of fragmentation in the single market and increasing legal certainty. Several EU Member States are considering or have put forward national legislation to enhance the safety of minors online: Italy, France, Norway, Greece, Austria, Poland and Belgium notified in 2025 and 2026[5] their draft legislation limiting access to certain digital services for minors under a certain age[6].

4. The Proposal draws on the recommendations of the Special Panel of experts to advise the Commission on the most appropriate approach for Europe on child safety online ('the Special Panel')[7]. In particular, the Panel advocates for an EU-wide access restriction, harmonised safety-by-design rules as well as proportionate, privacy-preserving age assurance systems[8]. It further recommends covering digital services beyond social media platforms, including app stores, AI companions and some video games and video-sharing platforms offering risky features[9].

5. The present Opinion of the EDPS is issued in response to a consultation by the European Commission of 17 September 2026, pursuant to Article 42(1) of EUDPR. The EDPS welcomes

[2] OJ L 295, 21.11.2018, p. 39.
[3] COM(2026) 681 final.
[4] SWD(2026) 681 final, Section 2.2 ('An insufficient level of protection for minors online').
[5] Member States have notified the EU Commission via the EU's Technical Regulation Information System (TRIS). They notified these drafts because EU law requires Member States to notify certain national technical rules to the European Commission before adoption. The obligation comes primarily from Article 5(1) Directive (EU) 2015/1535.
[6] Explanatory Memorandum of the Proposal, p. 1.
[7] The report of the Special panel, from July 2026, is available at https://commission.europa.eu/topics/digital-economy-and-society/special-panel_en.
[8] Explanatory Memorandum of the Proposal, p. 1.
[9] Explanatory Memorandum of the Proposal, p. 1.

the reference to this consultation in Recital 76 of the Proposal. The EDPS recommends correcting the reference to Article 42(1) EUDPR, as Recital 76 of the Proposal currently refers to Article 42(2) EUDPR.

2. General remarks

6. The EDPS strongly supports the Proposal's objectives of protecting children online and preventing regulatory fragmentation in the EU single market. Under Article 24(1) of the EU Charter of Fundamental Rights ('Charter'), children have the right to such protection and care as is necessary for their well-being. Certain online services pose growing risks to minors and protecting children must be a priority. The GDPR further recalls that children are a vulnerable group that merit specific protection[10].

7. As several Member States are advancing national legislation limiting minors' access to certain online services, an EU-level response is necessary to avoid fragmentation. The EDPS supports a harmonised European approach to the protection of minors in online services, to avoid the fragmentation that would result from the application of divergent Member State laws to the same or similar practices and services.

8. The EDPS welcomes the Proposal's emphasis on safety-by-design, an approach that has been consistently advocated by civil society and other stakeholders. Several requirements of the Proposal – for example on addictive design, recommender systems, safe settings and economic transactions[11] – concern practices that can also be harmful, unfair or even unlawful when applied to adults. While risks stemming from the design or functioning of online platform services are generally higher for children than for adults[12], both should be protected. This is particularly true for users that are vulnerable due to their age, credulity, disability, or any specific misfortune or circumstance of such gravity as to impair their judgment. Against this background, the EDPS recommends considering extending certain protections envisaged by the Proposal to all users of the covered services, regardless of their age.

9. The Proposal provides for several measures that interfere with the fundamental rights of children and adults, including freedom of expression, freedom of assembly, privacy and data protection. Any such interference must comply with Article 52 of the Charter. In addition to being the least intrusive among effective options, it must also be limited to what is necessary and proportionate to achieve the legitimate objective of protecting children online.

10. The protection of minors is an objective of legitimate general interest recognised by the Union[13], in addition to being a fundamental right under Article 24 Charter. The Commission Staff Working Document provides evidence of the risks for minors that the Proposal aims to address[14], referencing the Special Panel and impact assessments of previous legislative

[10] See Recitals (27) and (46) GDPR.
[11] Articles 9, 10, 11 and 13 of the Proposal.
[12] See EDPB Comments on the draft guidelines on protection of minors online under the Digital Services Act ('DSA'), p. 2.
[13] Judgment of the Court of Justice of 23 March 2023, *Booky.fi Oy*, Case C-662/21, ECLI:EU:C:2023:239, paragraph 41.
[14] Section 1.3, SWD (2026) 681. Section 2.2 of the SWD presents an overview of the risks minors face online (e.g., cyberbullying, exposure to harmful content, privacy infringements, grooming, disinformation, radicalisation), as well as the supporting evidence for each of them.

proposals, as well as ongoing enforcement actions under Regulation (EU) 2022/2065[15] (DSA)[16]. The EDPS welcomes the documentation and analysis of the risks at stake accompanying the Proposal. At the same time, the EDPS regrets that the external study on the impact of age assurance on the fundamental rights of children as well as adults commissioned by the Commission has not been finalised and taken into consideration prior to adoption of the Proposal.[17]

11. Regarding the scope of the interference, it is relevant that the Proposal covers many services that individuals (minors and adults) use on a regular basis, as it applies to any provider whose service or system is accessible to minors and falls within one of the following seven categories: (1) online social networking services ('OSNs'); (2) video-sharing platform services ('VSPs'); (3) software application stores; (4) online games; (5) operating systems; (6) AI companions; and (7) general conversational chatbots.[18]

12. In other words, the Proposal is not limited to online services that offer access to "adult" content only (e.g., online platforms that distribute pornographic content or provide gambling services). While several obligations would be applicable specifically to certain types of service providers under the Proposal, the Proposal renders the exemption from safety by design requirements contingent upon the use of age assurance in relation to each of the aforementioned services[19]. This approach *de facto* incentives the widespread deployment of age assurance mechanisms across diverse digital services accessed by individuals on a regular basis, including services that may be very important in their daily lives and for social participation[20]. At the same time, it does not address the underlying concerns regarding harms that persist after the specified age threshold has been reached.

13. As regards the nature of the interference, the EDPS welcomes the efforts of the Proposal to minimise the interference with fundamental rights, including the fundamental rights to privacy and data protection. This is evident where the Proposal requires taking into account minors' privacy and developing agency and autonomy when establishing guardian-controlled access to and use of certain services[21], but also where it requires age assurance to ensure a high level of accuracy, reliability, security, robustness, non-intrusiveness, privacy and data protection, and non-discrimination[22]. The EDPS very much welcomes the requirement that, in line with the European Data Protection Board ('EDPB') Statement on Age Assurance, solutions for age assurance and verification of parental responsibility may not enable the identification of users nor be used to locate, track, target, advertise to or profile them[23]. It is also welcomes that providers carrying out age assurance would be precluded from re-using that information for other purposes and that assurance solutions

[15] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L 277, 27.10.2022, pp. 1–102. Available at https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng
[16] Section 1.3.3, SWD (2026) 681.
[17] Section 1.3.2, SWD (2026) 681.
[18] Article 2(1) of the Proposal. There are certain categories currently excluded from the scope of the Proposal, namely: not-for-profit online encyclopaedias; not-for-profit educational and scientific repositories; services operated purely for educational purposes within schools; open-source software development platforms; scientific research services; and services developed by and for public authorities. There is no exemption for small and micro enterprises.
[19] Article 8(1) of the Proposal.
[20] Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms Adopted on 17 April 2024, paragraph 110.
[21] Articles 7(4) and 20(1)(e) and (f) of the Proposal.
[22] Article 27 Proposal.
[23] Article 28(1) of the Proposal. See EDPB Statement on Age Assurance, adopted on 11 February 2025, section 2.3.

should be based on state-of-the-art privacy-enhancing technologies including zero knowledge proof[24].

14. In addition to being the least intrusive among effective options, the selected measures must also be proportionate to achieve the legitimate objective of protecting children online and not exceed what is necessary[25]. The latter criterion (proportionality *strictu sensu*) requires, among others, that a balance is struck between the extent and nature of the interference and the necessity of interfering[26].

15. As stated by the EDPB, age assurance must respect individuals' fundamental rights, be implemented in a risk-based and proportionate manner and the best interests of the child should be a primary consideration[27]. Since the Proposal would de facto entail age assurance across a variety of services, the EDPS invites the co-legislators to carefully assess whether alternative measures (e.g., focusing on safety by design without age assurance or parental responsibility verification measures) may not equally be effective.

16. A measure that is routinely circumvented risks providing only the appearance of safety, rather than effective protection for children.[28] The EDPS therefore urges the co-legislature to also carefully consider the risks of circumvention of the measures that would be imposed via the Proposal[29].

17. The EDPS also considers it of utmost importance to take into account the principle that protection should not necessarily mean exclusion. Measures should enable children to benefit from the opportunities of the digital environment while managing risks, rather than imposing blanket restrictions that could undermine their rights, participation and development. The EDPS invites the co-legislators to carefully consider which specific functionalities of the services in scope of the Proposal effectively require use of age assurance as means to mitigate the risks minors are exposed to and which functionalities could also be sufficiently addressed by imposing safety by design measures that benefit all users, as well as possible alternative measures such as additional reporting functionalities for minors, complementary tools for guardians and digital literacy initiatives.

18. Where age assurance is shown to be necessary and proportionate, the EDPS considers that the use of privacy-enhancing technologies enabling selective disclosure and unlinkability of attributes, such as zero knowledge-proofs, is a key precondition to ensure compatibility between those age assurance requirements and Articles 7 and 8 of the Charter. It is therefore equally important to take into consideration the maturity and availability of the relevant technologies themselves, standardisation processes, widespread market adoption and social and personal accessibility[30]. Consequently, the entry into application of the

[24] Article 28(2) and (3) of the Proposal.
[25] See, in this respect, EDPS, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit; and EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data.
[26] Judgment of the Court of Justice of 9 November 2010, *Volker und Markus Schecke GbR and Hartmut Eifert*, Joined Cases C-92/09 and C-93/09, EU:C:2010:662, paragraph 86.
[27] EDPB Statement on Age Assurance, adopted on 11 February 2025, paragraphs 10 to 13. At paragraph 14, the EDPB notes that '*a service provider processing personal data to check the age of all their users when accessing all their content or services, even when the content or services are suitable for all audiences and devoid of any risk, would not pass the necessity and proportionality tests*'.
[28] EDPB Statement on Age Assurance, adopted on 11 February 2025, paragraph 22 concerning 'robustness'.
[29] For example, through virtual private networks (VPN), borrowed devices or accounts, or illicitly-obtained credentials.
[30] The age assurance requirements of the Proposal depend on infrastructure whose EU-wide availability and interoperability are not yet assured, notably electronic parental responsibility attestations and certified age verification solutions, including proof-of-age

relevant obligations of the Proposal should be aligned with demonstrable infrastructure readiness for age assurance and parental responsibility verification.

19. The EDPS notes that the Proposal would require the Commission to carry our reviews of its application to evaluate the impact of the Proposal on the respect for the right to freedom of expression and information[31]. Given the impact of the Proposal on other fundamental rights under the Charter, the EDPS recommends referring to those other fundamental rights – including privacy and data protection – in Article 42(1)(d) of the Proposal.

3. Interplay with EU data protection law

20. The EDPS welcomes that the Proposal would apply "without prejudice" to Regulation (EU) 2016/679[32] (GDPR) and Directive 2002/58/EC (ePrivacy Directive)[33]. Coherence between the Proposal and existing EU legislation is key to ensure legal certainty in scope of the Proposal. To this end, the EDPS recommends further clarifying the interaction of the Proposal with existing EU data protection legislation.

21. Article 6(5of the Proposal states that, 'where providers of services falling within scope of paragraph 1 process personal data pursuant to [Article 6(1)(a) GDPR], the provisions set out in [Article 6 of the Proposal] should apply in parallel to the age limits provided in Article 8 of that Regulation'. It is not clear why the clarification of the relationship with age checks pursuant to the Proposal with the requirements of Article 8 of the GDPR should be limited to providers of OSN and VSP services, as also other providers covered by the Proposal may be qualified as information society service providers and be bound by Article 8 of the GDPR.

22. Moreover, the EDPS is concerned that the Proposal and Article 8 of the GDPR could lead to a duplication of age assurance processes to be implemented by the providers in scope of the Proposal and covered by Article 8 GDPR. To avoid this and to ensure simplification and sound implementation of the requirements of both instruments, the EDPS recommends harmonising the age of consent in the context of information society services across the EU by amending Article 8 GDPR. In that case, the EDPS recommends adding Article 16 of the Treaty on the Functioning of the European Union ('TFEU') as a legal basis for the Proposal.[34]

23. The EDPS also recommends clarifying in a recital the relevant legal basis under Article 6(1) GDPR for providers that process personal data when complying with the requirements of the Proposal[35]. Processing that is required pursuant to a legal obligation or necessary for the performance of task in the public interest GDPR must, at least, determine the purpose(s) of the processing, meet an objective of public interest and be proportionate to the legitimate

issuance, certification and trusted lists. Further dependencies include zero knowledge proofs and the sharing of age signals by providers of operating systems.

[31] Article 42(1)(d) of the Proposal.

[32] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, pp. 1-88).

[33] Article 2(7) and Recital 51 of the Proposal.

[34] The EDPS understands that the Proposal does not further specify the requirements of the GDPR and hence did not rely on Article 16 TFEU, but only on Article 114 TFEU. This is despite the reference, in p. 59 of the SWD, that the Proposal would specify the application of GDPR principles of purpose limitation, data minimisation and data protection by design and by default.

[35] See in this regard also the EDPB Guidelines 3/2025 on the interplay between the DSA and the GDPR Version 2.0, Adopted on 17 September 2026, in particular paragraph 99.

aim pursued[36]. To ensure that such measures are proportionate, the EDPS recommends defining additional appropriate safeguards for the processing of personal data in the context of age assurance and verification of parental responsibility, such as defining a maximum retention period for the personal data collected in that context and further measures as specified under Section 8 of this Opinion.

4. Delayed creation and use of accounts for OSNs and VSPs

24. Under Article 6(1) of the Proposal, providers of online social networking services ('OSNs') and video-sharing platform services ('VSPs') may not allow minors under the age of 15 to create accounts that are considered to "pose a risk to the privacy, safety or security to the minors below the age of 15" in light of specific functionalities or systems[37].

25. Article 6(2) of the Proposal derogates from that rule where providers of OSN and VSPs can allow guardians to set up accounts for minors above the age of 13 years and below the age of 15 years with limited features ('limited accounts'), under certain conditions. Article 6(2)(c) of the Proposal raises challenges related to the minor's own right to privacy vis-à-vis their guardians. The need to respect the minor's agency[38] and privacy puts into question whether the pre-approval of new contacts by legal guardians[39] is necessary and proportionate. Questions also arise as to how this feature should be reconciled with the need to avoid "disproportionately restricting minors' rights" and "respecting minors' agency and privacy" as part of tools for guardians.[40] The EDPS therefore recommends removing he pre-approval of new contacts for minors above the age of 13 years under Article 6(2).

26. Providers of VSPs whose service is specifically designed for minors below the age of 13 years may exceptionally enable a guardian to allow a minor below the age of 13 years limited access to the service through the guardian's own account, upon certain conditions.[41] The EDPS welcomes that the age-appropriate features for minors below 13 years include that "personalisation features and recommender systems are turned off and cannot be activated" unless the provider in its risk assessment has demonstrated that their activation is "in the best interests of the minor and does not in any way negatively affect the minor's privacy, safety and security"[42]. The EDPS recommends extending this requirement to limited accounts under Article 6 Proposal.

5. Tools for guardians

27. Article 20 of the Proposal details the conditions for the tools for guardians. The tools are central to the Proposal's architecture, as they are mentioned as a key element of several requirements, including the delay in OSN and video platforms account creation.[43] The conditions for tools for guardians however also apply to providers of online games, AI companions and general conversational chatbots.

[36] Article 6(3) and Recital 41 GDPR.
[37] See Article 6(1) of the Proposal, which lists the criteria for considering a service as a risk to the privacy, safety or security of minors below 15 years of age.
[38] Article 18 of the Proposal.
[39] Article 6(2)(c) of the Proposal.
[40] Article 20(1)(e) and (f) of the Proposal.
[41] Article 7(1) of the Proposal.
[42] Article 7(1)(d) and (h) of the Proposal.
[43] See Articles 6(2)(a), 7(1)(b) and (4), 14(1)(d), 15(1)(d) and (3) and 16(4) of the Proposal.

28. While the EDPS welcomes that the Proposal recognises that compliance should not depend exclusively on guardians[44], it does give them a prominent role. Guardians should complement and not replace providers' responsibilities to ensure safe online spaces and should be provided with sufficient guidance on how different safety features can be used. Moreover, it is important that any solution that involves guardians after a verification of parental responsibilities takes into account the wide range of family configurations (separated, blended, same sex, fostered and unaccompanied minors, etc.), so as not to exclude or leave any minor unprotected.

29. The EDPS observes that the current provisions would grant providers extensive discretion in designing and implementing these tools, particularly regarding the requirements to avoid "disproportionately restricting minors' rights"[45] and "respecting minors' agency and privacy"[46]. Indeed, it is important to note that allowing the monitoring, by legal guardians, of minors' online activities may prevent a child from accessing a helpline or searching for sensitive information[47].

30. To ensure that tools for guardians remain limited to what is necessary and proportionate to protect minors, the EDPS recommends specifying to the greatest extent possible in the basic act the features of guardian tools to ensure minors' rights are respected and relying on delegated acts only for supplemental safeguards[48].

31. The EDPS welcomes the requirement that minors must be informed when guardian tools are used and receive real-time indications when monitoring functions are active[49], in line with the GDPR's transparency principle[50]. This requirement should be maintained and clearly articulated in the final text to ensure effective implementation (for example, by specifying the elements of information that should be conveyed to the minors about the use of the tools for guardians). It may be appropriate to give minors a right to object against the use of specific tools for guardians or at least extend their reporting rights under Article 19 of the Proposal if such is in the best interest of the child (e.g., when a parent is abusive towards the minor)[51].

6. Verification of parental responsibility

32. The Proposal would require providers to verify parental responsibility in order to enable the creation of guardian-controlled accounts[52] and implement the guardian tools[53]. The EDPS welcomes the explicit requirement that the verification process must be carried out in a privacy-preserving manner and may not lead to additional processing of personal data that

[44] Recital 43 Proposal.
[45] Art 20(1)(e) of the Proposal.
[46] Art 20(1)(f) of the Proposal.
[47] UN General comment No. 25 (2021) on children's rights in relation to the digital environment, paragraph 76. The same paragraph states that *"[p]arents' and caregivers' monitoring of a child's digital activity should be proportionate and in accordance with the child's evolving capacities*".
[48] Article 20(7) of the Proposal.
[49] Providers shall inform minors when a guardian tool is used (Article 20(1) of the Proposal) and notify them when monitoring tools are activated and used via a clear notification'(Recital 43 Proposal).
[50] Article 5(1)(a) GDPR.
[51] See EDPB Comments on the draft guidelines on protection of minors online under the Digital Services Act ('DSA'), p. 36.
[52] See Articles 6(3) and 7(3) of the Proposal.
[53] Article 26(1) of the Proposal. The Proposal refers to three possible verification methods: official databases, data the provider already holds, self-declaration (interim).

could enable the provider to determine the location of the adult or minor concerned or to track, target or profile the adult or minor[54].

33. At the same time, the EDPS notes that the privacy standard for verification under Article 26 Proposal appears different than under Article 28(3) of the Proposal on age assurance, as Article 26 of the Proposal does not refer to zero knowledge proof. Recital (49), however, confirms that such verification should also 'be carried out in a manner that respects data protection principles, particularly data minimization through the use of so-called 'zero knowledge proof''. In the interest of legal certainty, the EDPS reflecting the reference to data minimisation through zero knowledge proofs also in Article 26 of the Proposal, as it is an important data protection and security safeguard that should be binding on providers[55].

34. Article 26(1)(a) of the Proposal refers to freely accessible official online databases or online interfaces made available by Member States on the basis of which signals of parental responsibility can be obtained. Article 26(5) of the Proposal would empower the Commission to supplement the Proposal by specifying signals indicating parental responsibility pursuant to Article 26(1)(a).

35. The EDPS is concerned that if the delegated act under Article 26(5) of the Proposal is not in place when the Proposal enters into application, it may complicate verification processes across Member States. In any case, the relationship between the delegated act mentioned in Article 26(5) of the Proposal and the obligation for Member States to establish at least one privacy-preserving electronic means of attesting parental responsibility under Article 31(1) of the Proposal should be clearly articulated.

36. Article 26(1) of the Proposal provides for two alternative means for verifying parental responsibility, i.e. the use of 'signals' of parental responsibility and self-declaration. The EDPS is concerned that the Proposal does not clearly circumscribe the reliance on "signals" based on past engagement of the minor and the adult with the service[56]. Inference of parental responsibility on the basis of automated processing (e.g., use of profiling to infer/estimate the existence of a specific bond between users of the service), may involve high error rates and potential for discrimination in the access to the service. To ensure alignment with the GDPR, in particular with its principles of fairness, purpose limitation and data minimisation[57], the EDPS recommends clearly defining the specific necessary and proportionate "signals" that providers can rely on in the context of Article 26(1)(b) of the Proposal[58] and to prohibit any form of re-use for other purposes.

37. The EDPS also recommends discouraging reliance on self-declaration of parental responsibility as per Article 26(1)(c) of the Proposal. In this respect, the EDPS notes that self-declaration is not considered in Article 3(5)(i) of the Proposal as an appropriate means of age assurance and should consequently not be considered either as an appropriate means of verification of parental responsibility. There would be significant risks of circumvention

[54] Article 26(4) of the Proposal.
[55] It is also in line with the requirement under Article 31(1)(c) of the Proposal which provides that Member States shall make available privacy-preserving electronic means by which a guardian can obtain and present an attestation of parental responsibility and that those means 'shall not entail making any information on parental responsibility accessible to providers or to the public beyond the confirmation that parental responsibility exists'.
[56] Article 26(1)(b) of the Proposal.
[57] Article 5(1)(a), (b) and (c) GDPR.
[58] The proposal does not define "signals of the parental responsibility" (currently there is only a definition of "age signal" in Article 3(5)(j) of the Proposal).

should the possibility under Article 26(1)(c) be admitted, even if the provider is required to make "reasonable efforts" to verify the veracity of the declaration.[59] Self-declaration should not be considered a sufficient starting point nor interim measure[60], as it is not an effective and reliable form of verification of parental responsibility.

38. To avoid situations where minors in potentially vulnerable situations are excluded from using the services in scope, the Proposal should also require providers to check for instances of shared parental responsibility, minors in foster care, unaccompanied minors, as well subsequent changes and disputed claims of parental responsibility, against centralised official databases that exist or should be created at Member State level.

39. Given the experiences and competences of national competent authorities on this matter, the EDPS recommends formally consulting[61] both the EDPS and the EDPB on the delegated act pursuant to Article 26(5) of the Proposal.

7. Safety by design

40. The EDPS welcomes the Proposal's emphasis on safety-by-design. Although the focus of the Proposal is on the protection of minors, the EDPS underlines that these services should be designed to ensure safety for all users, including adults. Several requirements of the Proposal – for example on addictive design, recommender systems, safe settings and economic transactions – concern practices that can also be harmful, unfair or even unlawful in relation to adult users. While risks stemming from the design or functioning of online platform services are generally higher for children than for adults[62], both should be protected.

41. For example, it would not seem more acceptable for providers of the services in scope of the Proposal to use addictive design to encourage compulsive or excessive use by adults[63], or to design recommender systems in a manner that exploits their vulnerabilities[64], or to activate by default settings (e.g. geolocation and other tracking features or device access)[65] that would require consent to be lawful under Union data protection law[66].

42. In addition, the EDPS also considers that certain obligations could be made applicable to any service that is reasonably likely to be accessed by minors, without being contingent upon age assurance (e.g., Articles 8(1), 18 and 19 of the Proposal). The EDPS considers that providers should not be able to derogate from such obligations by virtue of having established that the recipient of the service or the user of the system is an adult. Article 8(1) of the Proposal should therefore be amended accordingly.

[59] Article 26(3) of the Proposal.
[60] It may also end up being used for a very long time, depending on how long Member States take to set up the official online databases or interfaces for verification.
[61] In accordance with Article 42(2) EUDPR.
[62] See EDPB Comments on the draft guidelines on protection of minors online under the Digital Services Act ('DSA'), p. 2.
[63] Cf. Article 9(1) of the Proposal.
[64] Cf. Article 10(2) of the Proposal.
[65] Cf. Article 11 of the Proposal.
[66] See in particular Article 5(3) of the ePrivacy Directive. See also European Data Protection Board (EDPB), Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, adopted on 12 March 2019, in particular at paragraph 40.

43. The EDPS underlines that many of the practices covered by the Proposal are already regulated by Union data protection law[67] and expresses the concern that by restricting certain practices in relation to minors alone, the Proposal risks inadvertently lowering protection for other users (notwithstanding the "without prejudice" clause in Article 2(7) of the Proposal). To avoid this, the EDPS invites the co-legislators to extend safety by design measures to all users (where applicable) and to clarify in a Recital that the fact that the Proposal prohibits certain practices for minors does not mean that they are lawful when applied to adult users.

44. The EDPS also recommends extending the prohibition established in Article 28(2) of the DSA on profiling-based advertising to all services covered by the Proposal that do not qualify as online platforms under the DSA (e.g., AI chatbots, online games, software application stores).

7.1. Obligations for OSNs and VSPs

45. In addition to the addictive design prohibition under Article 9 of the Proposal, the Proposal requires providers of OSNs and VSPs to adjust features of the recommender systems they use for minors[68], implement safe settings by default[69], put in place contact and interactions safeguards[70], as well as safeguards against excessive, impulsive or unwanted spending[71].

46. As regards the obligations for recommender systems under Article 10 of the Proposal, the EDPS supports the additional obligations for providers of OSNs and VSPs, which go beyond those applicable to very large online platforms (VLOPs) under Article 38 DSA and those derived from Article 28(1) DSA, as interpreted in the Commission's Guidelines on Article 28(1) DSA[72].

47. The EDPS recommends further clarifying Article 10(2)(b) and its relationship to Article 10(3)(b) of the Proposal. If the intention is to establish non-profiling-based recommender systems as the default option for minors – which the EDPS would welcome[73] - this should be state explicitly and Article 10(3)(b) of the Proposal should be amended to reinforce this approach. The EDPS also recommends including an explicit obligation for providers to honour the user's choices in relation to the recommender systems throughout their use of the service (i.e., across sessions)[74].

48. The EDPS welcomes the measures envisaged to ensure that settings are set, by default, to a high level of privacy, security and safety for minors[75]. It recalls, however, that compliance

[67] See the examples in paragraph 48 below.
[68] Article 10 of the Proposal.
[69] Article 11 of the Proposal.
[70] Article 12 of the Proposal.
[71] Article 13 of the Proposal.
[72] See Commission Guidelines on Article 28(1) DSA, Section 6.5.
[73] As recommended in the EDPS Opinion 1/2021 on the Proposal for a Digital Services Act, 10 February 2021, paragraphs 73 and 74.
[74] See EDPB Guidelines 3/2025 on the interplay between the DSA and the GDPR Version 2.0, Adopted on 17 September 2026, paragraph 94.
[75] Article 11(1) of the Proposal.

with Directive 2002/58/EC[76] (ePrivacy Directive) would already require that features such as geolocation, tracking, microphone and camera access, and access to contacts be activated only with the consent of the data subject and must, therefore, be switched off by default. Nonetheless, the EDPS welcomes that Article 11(2) of the Proposal would require such features, where activated by minors, to be deactivated at the end of each session.

49. The EDPS also welcomes the contact and interaction safeguards included in Article 12 of the Proposal[77]. At the same time, the EDPS observes that certain measures (e.g., under Article 12(3)(a) and (c) of the Proposal) would already be expected by controllers offering OSN and VSP to comply with Article 25 GDPR[78].

7.2. Obligations for AI companions and general conversational chatbots

50. Article 14 of the Proposal would oblige providers of AI companions and of general conversational chatbots to implement safety by design provisions related to addictive design, safe settings and transparency of commercial transactions set out by Article 9, 11 and 13 of Section II. It also provides specific rules tailored to these services.

51. The EDPS welcomes the proposed safeguards, including the prohibition on reusing information or analysis derived from a minor's prior interactions in subsequent interactions by default under Article 14(1)(b) of the Proposal. However, it recommends removing the phrase "by default" from this provision, as the existing exception for cases necessary to protect the minor's safety already provides sufficient flexibility without the need for this qualification.

52. The EDPS also welcomes the ban on automatic activation of certain features, as well as the requirement to provide opt-out options where these features form part of a broader service, as set out in Article 14(2)(a) and (c) of the Proposal. These measures represent important steps toward enhancing child protection in digital environments.

53. The EDPS notes that the compliance standard established in Article 14 of the Proposal differs from the standard of ensuring a high level of privacy, safety, and security for minors required under Article 28(1) DSA and other provisions of the Proposal. Article 14 of the Proposal sets a distinct standard focused on protecting minors' health, safety, fundamental rights, in line with the terminology used in Regulation (EU) 2024/1689[79] (AI Act), and overall well-being and development[80]. The EDPS notes that relying on different standards for compliance with different obligations may create unnecessary complexity for providers subject to this Proposal and recommends harmonising these requirements to ensure consistent and effective implementation.

---

[76] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), (OJ L 201, 31.7.2002, p. 37).
[77] Article 12 of the Proposal.
[78] See EDPB's Binding Decision 2/2022 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Meta Platforms Ireland Limited (Instagram) under Article 65(1)(a) GDPR, paragraphs 156-157.
[79] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj.
[80] Recitals 33 and 48; Articles 14(1) and 25(1)(e) of the Proposal.

54. The EDPS recommends clarifying the reference to "harms and emerging risks referred to in point (d)" in the context of Article 14(1)(f) of the Proposal, since point (d) of Article 14(1) does not explicitly address harms nor emerging risks. The EDPS also underlines that Article 14(1)(f) lacks clarity concerning the "serious incidents involving minors" that would require detection and response and recommends clarifying this aspect.

7.3. Obligations for providers of online games

55. Online games[81] would have their own specific obligations under Article 15(1) and (2) of the Proposal, including prohibitions on addictive design, the obligation to put in place safe settings, contact and interactions safeguards and tools for guardians, as well as safeguards to prevent the game from being used to entice minors to initiate contacts on other services.

56. The EDPS notes that online games are treated differently from OSN and video platforms and the Proposal does not require the same protections. Given the risks of excessive, impulsive or unwanted spendings by minors in online games, the EDPS recommends to at least require providers of online games to implement transparency measures and design safeguards related to economic transactions like the ones under Article 13 Proposal.

57. The EDPS is concerned that Article 15(2) of the Proposal may grant excessive discretion to providers of online games concerning the safeguards they put in place to comply. To avoid the risk that Article 15(2) of the Proposal results in widespread profiling and analysis of users' communications (including both written and verbal exchanges within gaming environments) and general monitoring of minors' in-game activities[82], the EDPS recommends clarifying in a Recital that the obligation should not entail such practices.

7.4. Age ratings and obligations of software application stores

58. Article 16 of the Proposal requires providers of software application stores to establish an age-rating system covering each application offered through their services and to prevent minors from accessing or purchasing applications that are inappropriate for their age. To give effect to those restrictions, providers must assess the age of recipients in accordance with Chapter V of the Proposal.[83] Article 16(3) of the Proposal further requires providers to respect minimum ages established under applicable Union law or national law that are higher than the minimum age established in the providers' age-rating system.

59. The EDPS welcomes the objective of ensuring age-appropriate access to software applications, as well as the obligation under Article 16(5) of the Proposal to make information on the methodology, criteria and sources underlying age-rating systems publicly available. It also welcomes the express recognition of higher age limits established under applicable EU or national law. Reliable age ratings are relevant to assess the

[81] This includes both video games and video gaming platforms (Article 3(5)(e)–(g) of the Proposal). According to Recital 12, it also covers free, paid and hybrid (in-app purchase) games, whether played locally or remotely. Games available only on physical media with no online component are excluded. A game that also has video-sharing features is treated as an online game. There is no exemption for micro or small enterprises. The general exclusions in Article 2(4) of the Proposal, such as purely educational services, still apply.
[82] Notwithstanding the stated aim not resulting in "general monitoring", as per Recital 7 of the Proposal.
[83] Article 16(4) of the Proposal.

suitability and proportionality of the processing of personal data undertaken to enforce those ratings. An inaccurate rating may undermine the protection of minors or result in unnecessary restrictions and associated processing of personal data via age assurance.

60. The EDPS considers that the responsibility of providers of software application stores for enforcing access restrictions should be distinguished from the assessment of the age-appropriateness of an application. Entrusting those providers with considerable discretion over that assessment, without sufficient independent scrutiny, may undermine the reliability and consistency[84] of the thresholds subsequently enforced through age assurance. While the EDPS understands that codes of conduct under Article 17 of the Proposal could contribute to defining common criteria in this context, it is not a given that these codes of conduct will be in place when the obligations under Article 16 start applying.

61. The EDPS therefore recommends amending Article 16 to require providers of software application stores to use ratings issued or validated under common criteria by independent or publicly recognised classification bodies. Publishers should provide complete and accurate information on the relevant content and functionalities of their applications and notify material changes to those bodies. The Proposal should also expressly preserve national classification and listing powers concerning applications that may be harmful to minors, together with the associated distribution restrictions, insofar as these comply with Union law.

62. The EDPS also suggests that Article 16 of the Proposal specifies that the age ratings to be established for OSN and VSP applications that pose a risk to the privacy, safety or security of a minor should, in principle, be consistent with the minimum ages for account creation pursuant to Article 6(1) and (2) of the Proposal.

7.5. Codes of Conduct on age rating and online games

63. Article 17(1) of the Proposal would oblige the Commission to encourage and facilitate the development of Union-level codes of conduct concerning age-rating systems and online games. These codes should contribute, among other things, to defining common assessment criteria, consistent application of ratings, independent redress and regular monitoring.[85] Article 17(3) of the Proposal would require the Commission to assess the adequacy of the codes and regularly monitor and evaluate the achievement of their objectives.

64. The EDPS welcomes the involvement of relevant authorities, organisations representing minors and their guardians, and civil society in developing these codes. Where a code would specifically address measures involving the processing of personal data[86], the EDPS recommends expressly requiring consultation of the EDPB. The assessment of a code by the Commission under Article 17(3) of the Proposal should be without prejudice to the tasks and powers of data protection supervisory authorities and should not, in itself, establish compliance with the GDPR. Similar considerations apply in relation to codes of conduct under Article 23 of the Proposal.

[84] However, Articles 16 and 17 of the Proposal do not sufficiently ensure that equivalent versions of the same application receive consistent, independently validated ratings across distribution channels.
[85] Article 17(2) of the Proposal.
[86] For example, pursuant to Article 17(2)(f) of the Proposal when it comes to defining appropriate measures and methodologies to give effect to the obligations laid down in Article 15(1), (2), (3) and (4).

65. The EDPS further recommends strengthening the governance arrangements accompanying the Commission's assessment and monitoring functions. The Proposal should specify responsibility for independently monitoring adherence by participating providers, investigating complaints and addressing non-compliance. Articles 40 and 41 GDPR provide a useful reference in this respect, distinguishing approval of a code, monitoring by an accredited body and supervisory oversight. The Proposal should provide for corrective measures and, where appropriate, withdrawal of a finding that a code is adequate to demonstrate compliance.

7.6. Agency of minors and child-friendly reporting and support tools for minors

66. The EDPS welcomes Articles 18 and 19 of the Proposal which establish important obligations for providers of OSNs, VSPs, online games, AI companions, and general conversational chatbots to provide minors with clear information, control tools, and reporting mechanisms. These provisions enhance minors' ability to manage their online experiences, and the EDPS recommends that they are included as general safety by design obligations applicable to all providers covered by the Proposal. The EDPS notes that obligations like the ones under Articles 18 and 19 of the Proposal would be relevant for all providers of online platforms[87] more broadly and for the protection of all users of online services (not only minors).

67. While generally supportive of these measures, the EDPS expresses concern about the potential implications of Article 19(4)(c) of the Proposal which requires displaying warning messages where minors are likely to publish or be exposed to content or interactions presenting a risk to their privacy, safety or security[88]. Absent further precisions or clarifications, this provision could inadvertently incentivise extensive profiling or even analysis of minors' private communications. The EDPS therefore recommends either further specifying well-defined and proportionate measures for implementing this obligation or limiting the duty to display warnings to cases where minors are likely to be exposed to harmful content rather than when they might be about to share it.

8. Age Assurance

68. Chapter V of the Proposal contains both general requirements and specific safeguards for age assurance. Article 27 of the Proposal would require solutions to provide a high level of accuracy, reliability, security, robustness, non-intrusiveness, privacy, data protection and non-discrimination. Article 28 of the Proposal would limit the processing of personal data,

[87] Article 3(i) DSA defines 'online platform' as a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public, unless that activity is a minor and purely ancillary feature of another service or a minor functionality of the principal service and, for objective and technical reasons, cannot be used without that other service, and the integration of the feature or functionality into the other service is not a means to circumvent the applicability of this Regulation.
[88] See also in Recital 40 of the Proposal: "To ensure that minors are aware of the risks in the online environment, they should be informed of the specific risks prior to posting content or enhancing the visibility of certain content such as reposting content posted by other recipients. To that end, providers of online social networking services, of video-sharing platform services, AI companions, general conversational chatbots, and of online games, should, where appropriate, implement warning messages or other suitable measures aimed at informing minors before they undertake any actions."

prohibit specified uses of age assurance information and require the use of zero knowledge proofs.

69. The EDPS very much welcomes Articles 28(1) and (2) of the Proposal, which reflect the principles of data minimisation and purpose limitation and support a data protection by design and by default approach.[89] The EDPS very much welcomes the requirement that, in line with the EDPB Statement on Age Assurance, solutions for age assurance and verification of parental responsibility may not enable the identification of users nor be used to locate, track, target, advertise to or profile them[90]. It is also welcomes that providers carrying out age assurance would be precluded from re-using that information for other purposes.

70. The EDPS also very much welcomes the requirement to use zero knowledge proofs in Article 28(3) of the Proposal. Such cryptographic methods can enable a person to demonstrate compliance with an age threshold without disclosing the underlying age or identity information to the service provider. However, the Proposal does not define this concept. The EDPS recommends introducing a definition of 'zero knowledge proof' in Article 3 of the Proposal, reflecting its established cryptographic meaning: a proof that establishes the validity of a statement (e.g., confirmation of being above a certain age or between a certain age range) without revealing information beyond what follows from the statement itself (e.g., the precise date of birth).

71. The EDPS recalls that age assurance may affect not only the rights to privacy and the protection of personal data, but also (depending on its consequences) other fundamental rights, including non-discrimination and freedom of expression and information. The protection of children must therefore be pursued through measures whose effectiveness, necessity and proportionality can be demonstrated, taking account of their effects on all persons required to undergo age assurance. The EDPB has similarly emphasised the need for a proportionate approach that respects the full range of fundamental rights[91].

72. The EDPS recommends expressly specifying that providers of the services for which age assurance is to be performed must not retain a recipient's precise age or date of birth for that purpose[92]. Providers should receive and, where permitted, retain only the minimum information necessary to establish compliance with the relevant threshold.

73. Article 28(4) of the Proposal would permit most providers covered by the Proposal to retain an age signal at account level solely to avoid repeated age assurance. While acknowledging the potential convenience of such retention, recipients should not be required to create an account solely to enable retention of an age signal. Moreover, repeated presentation of privacy-preserving unlinkable proofs may be preferable to persistent account-based storage. The Proposal should therefore make account creation and retention of age signals dependent on an express request by the recipient of the service, rather than leaving the decision solely to the provider. This option should be free of charge, accompanied by an equally accessible means of withdrawing the request and deleting or updating the signal, and limited to the information and retention period strictly necessary.

[89] Article 5(1)(b) and (c) and Article 25 GDPR.
[90] Article 28(1) of the Proposal. See EDPB Statement on Age Assurance, adopted on 11 February 2025, section 2.3.
[91] EDPB Statement on Age Assurance, adopted on 11 February 2025, paragraph 4.
[92] EDPB Guidelines 3/2025 on the interplay between the DSA and the GDPR Version 2.0, Adopted on 17 September 2026, paragraph 101.

74. The EDPS welcomes Article 28(5) of the Proposal, which would require providers to implement necessary technical and organisational measures to comply with age assurance data protection provisions. This specification effectively underscores the accountability requirements for providers. The EDPS also welcomes the Proposal's explicit exclusion of self-declaration methods for age assurance[93], as the EDPB has previously expressed serious doubts about their effectiveness in high-risk processing contexts[94].

8.1. Alternative age assurance methods

75. Article 29(1)-(3) of the Proposal would require providers of OSNs and VSPs to use exclusively certified EU age verification solutions relying on third-party proof-of-age attestations for the purpose of complying with Article 6 (delayed creation and use of accounts). By contrast, Article 29(4) of the Proposal would permit alternative age-assurance solutions for compliance with Articles 8(1) (general obligation of safety by design) and 16(2) and (3) (obligations for providers of software application stores), provided that providers demonstrate compliance of those solutions with Articles 27 and 28. Article 30(3)(a) would empower the Commission to specify requirements for those alternatives through delegated acts.

76. The EDPS recommends that providers are required to offer several viable alternatives for age assurance, rather than relying on a single method[95]. On this note, the EDPS recalls that the use of European Digital Identity Wallets for age assurance purposes must remain voluntary, in accordance with Article 5a(15) of Regulation (EU) No 910/2014, as amended[96]. Given that fully automated age assurance can produce legal or similarly significant effects, it is also important to provide for safeguards enabling users to obtain human intervention, express their point of view and contest such automated decisions[97]. The EDPS recommends enhancing Article 29(5) of the Proposal to make express reference to the possibility to seek human review and the possibility of providing age assurance through other means.

77. The EDPS welcomes the requirement that alternative solutions comply with the same substantive safeguards concerning accuracy, reliability, non-discrimination, data minimisation and purpose limitation, including the requirement to use zero knowledge proofs[98]. However, the definition of age assurance expressly encompasses age estimation, and the Proposal does not explain how estimation methods would meet those safeguards.

78. Generally speaking, age estimation is less precise than age verification and it may also entail a higher degree of interference with users' fundamental rights to privacy and data protection[99]. For example, estimating age from facial images or on the basis of derived or inferred data involves intrusive processing and yield uncertain results. Incorrect estimates

[93] Article 3(5)(i) of the Proposal.
[94] See para 228 of the Binding Decision 2/2023 on the dispute submitted by the Irish SA regarding TikTok Technology Limited (Art. 65 GDPR), adopted on 2 August 2023.
[95] As suggested in paragraphs 17 and 22 (on 'accessibility') of the EDPB Statement on Age Assurance, adopted on 11 February 2025.
[96] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework, OJ L, 2024/1183, 30.4.2024, available at http://data.europa.eu/eli/reg/2024/1183/oj.
[97] EDPB Statement on Age Assurance, adopted on 11 February 2025, paragraphs 27 to 30.
[98] Article 29(4) of the Proposal.
[99] EDPB Comments on the draft guidelines on protection of minors online under the Digital Services Act ('DSA'), p. 2.

may expose minors to harmful services or unjustifiably restrict access by eligible recipients. Such methods would not be compatible with Article 27 and Article 28 of the Proposal[100]. Reliance on insufficiently trustworthy registers or documents would likewise undermine the reliability of the resulting age signal[101].

79. Therefore, in line with the views previously expressed by the EDPB[102], the EDPS recommends expressly excluding algorithmic age estimation methods and other intrusive practices from the age assurance solutions permitted under the Proposal. This substantive safeguard should be established in the Proposal itself, rather than left to subsequent specification through the delegated acts envisaged in Article 30(3)(a) of the Proposal.

8.2. Age signals provided by providers of operating system

80. Article 29(6) of the Proposal would require providers of operating system, after obtaining the user's consent, to enable the sharing of an age signal with providers covered by the Proposal where that signal is required for compliance. Age signals would need to be obtained in compliance with Article 27 of the Proposal. Article 30(3)(b) would empower the Commission to adopt delegated acts specifying requirements for secure, privacy-preserving and interoperable sharing.

81. It is not immediately apparent in which context the providers of operating systems would collect age signals, as they would not be required to conduct age assurance pursuant to the Proposal nor are they covered by Article 28 of the DSA. If the goal of the Proposal is to establish an obligation for providers of operating systems to carry out age assurance at the request of the user, it should clearly state such obligation and provide for an appropriate justification.

82. In any event, the EDPS considers that the safeguards applicable to the collection and sharing of age signals by providers of operating systems should be further specified. The EDPS recommends expressly providing that providers of operating system must comply with both Articles 27 and 28 when obtaining, retaining and sharing age signals. Equivalent safeguards should apply to recipients of those signals. Sharing should disclose only the information strictly necessary for the applicable age threshold and must not create additional means of identification, tracking, profiling or linking a person's activities across services. Users should have an accessible alternative means of demonstrating their age, without detriment if they refuse or withdraw consent to sharing. The delegated act under Article 30(3)(b) of the Proposal should specify the technical and organisational arrangements implementing these safeguards.

8.3. Specifications and governance of the EU Age Verification Scheme

83. Article 30(2) of the Proposal would require the Commission to adopt implementing acts specifying the functioning of the EU Age Verification Scheme, including requirements for solutions, proof-of-age attestations and their providers. Article 30(3) would provide for

[100] See also recitals (50) and (51) of the Proposal.
[101] A zero-knowledge proof of an estimated result does not establish either the accuracy of that result or the necessity and proportionality of the processing used to generate it.
[102] EDPB Comments on the draft guidelines on protection of minors online under the Digital Services Act ('DSA'), p. 12.

delegated acts concerning alternative age assurance solutions and the sharing of age signals by operating system providers.

84. The EDPS welcomes the express references to data minimisation, purpose limitation, security, proportionality and interoperability with European Digital Identity Wallets in Article 30(2) of the Proposal. To ensure legal certainty, the implementing acts should clearly identify how their requirements relate to those already established under the European Digital Identity Framework. Requirements already governed by that framework should not be duplicated or contradicted; additional specifications should address the particular needs of age verification under the Proposal.

85. The EDPS recommends requiring the implementing and delegated acts necessary for compliance to be adopted sufficiently in advance of the application of the corresponding obligations to allow their effective implementation. Their adoption should be accompanied by timely availability of the required certification arrangements and technical infrastructure. The EDPS further recommends expressly providing for consultation of the EDPB and the EDPS on measures adopted under Article 30(2) and (3) that concern the processing of personal data under Article 42(2) EUDPR.

8.4. Availability and accessibility of verification solutions

86. Article 31 of the Proposal would require Member States to establish privacy-preserving electronic means of obtaining and presenting attestations of parental responsibility and to ensure the availability of at least one certified EU age-verification solution. The EDPS welcomes the requirement that these means and solutions be available free of charge.[103] It also welcomes the safeguards limiting disclosure of information concerning parental responsibility and the requirement to provide alternative procedures where standard civil status documentation is unavailable[104].

87. Article 31(2) of the Proposal expressly addresses the accessibility of electronic means for demonstrating parental responsibility, including for persons with disabilities, limited digital access or skills, and persons in vulnerable situations. The EDPS recommends extending equivalent requirements to the age verification solutions and means of obtaining proof-of-age attestations envisaged in Article 31(4) and (5) of the Proposal. Lack of suitable equipment, documentation or digital skills should not oblige individuals to accept more intrusive processing or prevent them from accessing services for which they are eligible.

88. The EDPS expressly providing that Member States are required to establish a privacy-preserving electronic means by which a guardian can obtain and present an attestation of parental responsibility, as well as ensure the availability of proof-of-age attestation and an EU age verification solution at the latest by the date of application of the Proposal.

8.5. Existing accounts

89. Article 32(2) of the Proposal would permit providers covered by Article 6(1) to not carry out age verification where they can establish, with a high degree of confidence, that the

[103] Article 31(1)(b) of the Proposal.
[104] Article 31(1)(c) and (3) of the Proposal.

recipient has reached the applicable minimum age. Similarly, Article 32(3) of the Proposal would exempt providers covered by Article 8(1) and providers of software application store from age assurance requirements if they can establish, with a high degree of confidence that the recipient of the services is not a minor.

90. The EDPS welcomes the objective of avoiding unnecessary repeated checks. However, the circumstances and evidence capable of supporting the conclusion that a recipient of the service is above a certain age or is not a minor should be specified more clearly in Article 32. The indications in Recitals 61 and 62 of the Proposal do not clearly delineate the information that providers may use or the processing they may undertake for that purpose.

91. The EDPS recommends specifying objective, verifiable criteria for reliance on these derogations, together with requirements to document and demonstrate their reliability. The Proposal should expressly preclude reliance on profiling or biometric analysis and clarify that the exceptions do not authorise additional collection or repurposing of personal data in a manner which is incompatible with Articles 27 and 28 of the Proposal. Where the available evidence does not establish the relevant threshold with the required confidence, providers should offer a compliant age assurance method.

9. Competences, supervision and enforcement

92. The Proposal designates competent authorities under the DSA and the AI Act as responsible for supervising compliance, depending on the nature of the services provided[105]. Member States would be required to designate an authority for supervising providers of online games that are not considered as online platforms under the DSA[106].

93. Article 34(6) of the Proposal confirms that data protection supervisory authorities under the GDPR shall be competent to monitor the processing of personal data necessary to comply with the Proposal, and in particular Articles 27, 28 and 29. While recognising that Article 27-29 of the Proposal are particularly relevant from a data protection perspective, the EDPS recommends expressly clarifying, by way of a recital, that the Proposal does not affect the competence of data protection supervisory authorities to apply and enforce the GDPR in the context of practices that are covered by the Proposal (e.g., personal data processing in recommender systems or default settings). The EDPS also recommends specifying that Chapters VI and VII of the GDPR shall apply *mutatis mutandis*.

94. Article 34(7) of the Proposal provides that Member State authorities shall not take decisions which run counter to a decision adopted by the Commission under this Regulation. The EDPS understands that this reference to competent authorities refers to authorities designated in accordance with the DSA and the AI Act. While all supervisory authorities are bound to a duty of sincere cooperation and to ensure coherence in the application of EU law[107], the Proposal should not interfere with the independence of data protection authorities as guaranteed by Article 8 of the Charter and 16 TFEU.

[105] Article 34(1) and (2) of the Proposal.
[106] Article 34(5) of the Proposal.
[107] Article 4(2) of the Treaty on European Union, as interpreted in the Judgment of the Court of Justice of the European Union of 4 July 2023, *Meta Platforms Inc. v Bundeskartellamt*, C-252/21, EU:C:2023:537, paragraph 53.

95. The EDPS welcomes that Article 34(7) of the Proposal provides that competent authorities are to cooperate closely and coordinate their actions. At the same, the EDPS notes that the provision does not specifically refer to data protection supervisory authorities, notwithstanding their role under Article 34(6). In line with the EDPS's previous Opinion on the DSA Proposal[108] and the recent call of the EDPB for an EU-level legal basis for cross-regulatory cooperation[109], the EDPS strongly recommends establishing a legal basis for cooperation between the various competent authorities, including data protection authorities, including for the exchange of confidential information obtained in the context of any audits and investigations.

10. Conclusions

96. In light of the above, the EDPS makes the following recommendations:

(1) To ensure that requirements entailing age assurance and verification of parental responsibility comply with requirements of necessity and proportionality under Article 52 Charter and to ensure that they are deployed in a risk-based and proportionate manner, taking into account the best interests of the child;

(2) To carefully consider which specific features of the services in scope of the Proposal effectively require use of age assurance as means to mitigate the risks for minors in particular and which risks could be effectively addressed by imposing only safety by design measures that benefit all users;

(3) To ensure that age assurance and parental verification obligations only enter into application once the privacy-preserving solutions envisaged by Proposal are available across the EU;

(4) To clarify and simplify the relationship between the Proposal and Union law on the protection of personal data by clarifying the legal basis the processing of personal data and by harmonising the age of consent for personal data processing in information society services across the EU;

(5) To consider whether requirements on addictive design, recommender systems, safe settings and economic transactions should be extended to services covered in the Proposal other than online social networking and video-sharing platform services;

(6) To specify a maximum retention period for the personal data collected in the context of the age assurance and verification of parental responsibility;

(7) To remove the pre-approval of new contacts for minors above the age of 13;

[108] EDPS Opinion 1/2021 on the Proposal for a Digital Services Act, 10 February 2021, paragraphs 87 to 89.
[109] EDPB calls for legal basis for cross-regulatory information sharing, 17 July 2026.

(8) To extend the measures under Article 7(1)(h) regarding the personalisation features and recommender systems to limited accounts under Article 6;

(9) To expand the prohibition established in Article 28(2) of the DSA on profiling-based advertising to all services covered by the Proposal;

(10) To clarify that a non-profiling-based recommender system should be the default option for minors and require providers to honour the user's choices throughout their use of the service;

(11) To specify the "harms and emerging risks" mentioned in the provision and by defining "serious incidents involving minors" that would require detection and response under Article 14(1)(f);

(12) To require providers of online games to implement transparency measures and design safeguards related to economic transactions;

(13) To clarify that the obligation set out Article 15(2) of the Proposal should not result in profiling or analysis of users' communications and general monitoring of minors' in-game activities;

(14) To require providers of software application stores to use age ratings issued or validated under common criteria by independent or publicly recognized classification bodies;

(15)To specify that age ratings to be established for OSN and VSP applications that pose a risk to the privacy, safety or security of a minor should, in principle, be consistent with the minimum ages for account creation pursuant to Article 6(1) and (2) of the Proposal.

(16) To provide for consultation of the EDPB where a code of conduct under Articles 17 or 23 would specifically address measures involving the processing of personal data;

(17) To include the obligations of Articles 18 and 19 of the Proposal as general safety by design obligations applicable to all providers covered by the Proposal;

(18) To specify well-defined, proportionate, and targeted measures to comply with Article 19(4)(c);

(19) To consider giving minors a right to object against the use of specific tools for guardians or at least enable them to report misuse of the tools for guardians;

(20) To incorporate a reference to data minimisation through zero knowledge proofs in Article 26 of the Proposal;

(21) To clearly define the necessary and proportionate "signals" that providers can rely on to verify parental responsibility and to exclude reliance on self-declaration;

(22)To add a definition of 'zero knowledge proof' in Article 3 of the Proposal;

(23) To ensure that retention of an age signal under Article 28(4) of the Proposal would depend on an express request by the recipient of the service;

(24) To ensure that providers offer multiple viable alternatives for age assurance and that users are able to obtain human intervention and express their point of view regarding outcomes;

(25)To allow age estimation only where sufficient guarantees and safeguards are in place to ensure they do not lower the level of privacy, safety and security of individuals;

(26) To clarify whether providers of operating systems are obliged to collect age signals and, if so, why;

(27)To further specify safeguards for the collection and sharing of age signals by providers of operating systems;

(28) To provide for consultation of the EDPS and the EDPB on draft implementing and delegated acts adopted under Article 26(5), Article 30(2) and (3) and to ensure that the specifications are in place prior to entry into application;

(29) To extend the accessibility of electronic means for demonstrating parental responsibility under Article 31(2) of the Proposal also to Article 31(4) and (5) of the Proposal;

(30) To further specify the circumstances and evidence capable of giving a provider a high degree of confidence that a recipient of the service is above a certain age or is not a minor and to expressly preclude reliance on profiling or biometric analysis;

(31) To clarify that the derogations from the obligation to carry out age assurance under Article 32(2) and (3) of the Proposal do not authorise additional collection or repurposing of personal data in a manner which is incompatible with Articles 27 and 28 of the Proposal;

(32) To establish a legal basis for cooperation between the various competent authorities under the Proposal, including for the exchange of confidential information obtained in the context of any audits and investigations; and

(33) To refer to the fundamental rights to privacy and data protection the review clause of Article 42(1)(d) of the Proposal.

Brussels, 12 November 2026

(e-signed)
Wojciech Rafał WIEWIÓROWSKI