EUROPEAN
COMMISSION

Brussels, XXX
[…](2025) XXX draft

ANNEX

SENSITIVE*

ANNEX

to the

Communication to the Commission

Approval of the content on a draft Communication from the Commission on Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28(4) of Regulation (EU) 2022/2065

* Distribution only on a 'Need to know' basis - Do not read or carry openly in public places. Must be stored securely and encrypted in storage and transmission. Destroy copies by shredding or secure deletion. Full handling instructions https://europa.eu/!db43PX

1 INTRODUCTION

1. Online platforms are increasingly accessed by minors ([1]) and can provide several benefits to them. For example, online platforms may provide access to a wealth of educational resources, helping minors to learn new skills and expand their knowledge. Online platforms may also offer minors opportunities to connect with others who share similar interests, helping minors to build social skills, confidence and a sense of community. By playing on and exploring the online environment, minors can also foster their natural curiosity, engaging in activities that encourage creativity, problem solving, critical thinking, agency and entertainment.

2. There is, however, wide consensus among policy makers, regulatory authorities, civil society, researchers, educators and guardians ([2]) that the current level of privacy, safety and security online of minors is often inadequate. The design and features of the wide variety of online platforms and the services offered by providers of online platforms accessible to minors may create risks to minors' privacy, safety and security and exacerbate existing risks. These risks include, for example, exposure to illegal content ([3]) and harmful content, as well as unwanted contact that undermines minors' privacy, safety and security or that may impair the physical or mental development of minors. They also include cyberbullying or contact from individuals seeking to harm minors, such as those seeking to sexually abuse or extort minors, human traffickers and those seeking to recruit minors into criminal gangs or promote radicalisation and violent extremism. Minors may also face risks as consumers as well as risks related to extensive use or overuse of online platforms and exposure to inappropriate or exploitative practices, including in relation to gambling and gaming. The increasing integration of artificial intelligence ("AI") chatbots and companions into online platforms as well as AI driven deep fakes may also affect how minors interact with online platforms, exacerbate existing risks, and pose new ones that can negatively

(1) In the present guidelines, 'child', 'children' and 'minor' refer to a person under the age of 18.

(2) In the present guidelines, 'guardians', refer to persons holding parental responsibilities.

(3) Illegal content includes but is not limited to content depicting illicit drug trafficking, terrorist and violent extremist content and child sexual abuse material. What constitutes illegal content is not defined by the Regulation (EU) 2022/2065 (the Digital Services Act) but by other laws either at EU level or at national level.

affect a minor's privacy, safety and security ([4]). These risks can originate from the direct experience of the minor with the platform and/or from the actions of other users on the platform.

3. These guidelines aim to support providers of online platforms in addressing these risks by providing a set of measures that the Commission and the Digital Services Coordinators consider will help providers to ensure a high level of privacy, safety and security of minors on their platforms, which will contribute to safeguard minors' overall well-being. For instance, making minors' accounts more private will, inter alia, help providers of online platforms reduce the risk of unwanted or unsolicited contact. Implementing age assurance measures ([5]) may, inter alia, help providers reduce the risk of minors being exposed to services, content, conduct, contacts or commercial practices that undermine their privacy, safety and security. Adopting these and other measures – on matters ranging from recommender systems and governance to user support and reporting – may help providers of online platforms make online platforms safer, more secure and more privacy preserving for minors.

2 SCOPE OF THE GUIDELINES

4. It is in the light of the aforementioned risks that the Union legislature enacted Article 28 of Regulation (EU) 2022/2065 of the European Parliament and the Council ([6]). Paragraph 1 of this provision obliges providers of online platforms accessible to minors to put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors, on their service. Paragraph 2 prohibits providers of online platform from presenting advertisements on their interface based on profiling, as defined in Article 4, point (4), of Regulation (EU) 2016/679, using personal data of the recipient of the service when they are aware with reasonable certainty that the recipient of the service is a minor. Paragraph 3 specifies that compliance with the obligations set out in Article 28 shall not oblige providers of online platforms accessible to minors to process additional personal data in order to

(4) A typology of risks to which minors are exposed when accessing online platforms, based on a framework developed by the OECD, is included in Annex I to these guidelines.

(5) See section 6.1 on age assurance.

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

assess whether the recipient of the service is a minor. Paragraph 4 provides that the Commission, after consulting the Board, may issue guidelines to assist providers of online platforms in the application of paragraph 1.

5. These guidelines describe the measures that the Commission considers that providers of online platforms accessible to minors should take to ensure a high level of privacy, safety and security for minors online, in accordance with Article 28(1) of Regulation (EU) 2022/2065 of the Council and the Parliament. The obligation laid down in that provision is addressed to providers of online platforms whose services are accessible to minors ([7]). Recital 71 of that Regulation explains that "[a]*n online platform can be considered accessible to minors when its terms and conditions permit minors to use the service, when its service is directed at or predominantly used by minors, or where the provider is otherwise aware that some of the recipients of its service are minors*".

6. As regards the first scenario described in that recital, the Commission considers that a provider of an online platform cannot solely rely on a statement in its terms and conditions excluding minors, to argue that the platform is not accessible to them. If the provider of the online platform does not implement effective measures to actually prevent minors from accessing its service, it cannot claim that its online platform falls outside the scope of Article 28(1) of Regulation (EU) 2022/2065 based on that declaration. For example, providers of online platforms that host and disseminate adult content, such as online platforms disseminating pornographic content, and therefore restrict, in their terms and conditions, the use of their service to users over the age of 18 years, will be considered accessible to minors within the meaning of Article 28(1) of Regulation (EU) 2022/2065 when no effective measures have been taken to prevent minors from accessing the service.

7. As regards the third scenario, recital 71 of Regulation (EU) 2022/2065 explains that one example of a situation in which a provider of an online platform should be aware that some of the recipients of its service are minors is where that provider already processes the personal data of those recipients revealing their age for other purposes,

(7) Article 3 of Regulation (EU) 2022/2065 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.

such as during registration, and this reveals that some of those recipients are minors. Other examples of situations in which a provider can reasonably be expected to know that minors are recipients of its service include those in which the online platform is known to appeal to minors; the provider of the online platform offers similar services to those used by minors; the online platform is promoted to minors; the provider of the online platform has conducted or commissioned research, or independent research has identified minors as recipients of the services.

8. Pursuant to Article 19 of Regulation (EU) 2022/2065, the obligation laid down in Article 28(1) of Regulation (EU) 2022/2065 does not apply to providers of online platforms that qualify as micro or small enterprises, except where their online platform has been designated by the Commission as a very large online platform in accordance with Article 33(4) of that Regulation ([8]).

9. Other provisions of Regulation (EU) 2022/2065 are also aimed at ensuring the protection of minors online ([9]). These include, inter alia, several provisions in Section 5 of Chapter III of Regulation (EU) 2022/2065, which imposes additional obligations on providers of very large online platforms ("VLOPs") and very large online search engines ("VLOSEs") ([10]). To the extent that the obligations expressed in those provisions also relate to the privacy, safety and security of minors within the meaning of Article 28(1) of Regulation (EU) 2022/2065, these guidelines build on these provisions. These guidelines do not aim to interpret those provisions and providers of VLOPs should not expect that adopting the measures described below, either partially or in full, suffices to ensure compliance with their obligations under Section 5 of Chapter III of Regulation (EU) 2022/2065, as those providers may need to put in place

(8) Recommendation 2003/361/EC defines a small enterprise as an enterprise which employs fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million. A microenterprise is defined as an enterprise which employs fewer than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 2 million. The Commission recalls here Recital 10 of Regulation (EU) 2022/2065 which states that Regulation (EU) 2022/2065 is without prejudice to Directive (EU) 2010/13. The aforementioned Directive requires all video-sharing platform (VSP) providers, whatever its qualification as micro or small enterprises, to establish and operate age verification systems for users of video-sharing platforms with respect to content which may impair the physical or mental development of minors.

(9) This includes the obligations contained in the following provisions of Regulation (EU) 2022/2065: Article 14 on Terms and Conditions, Articles 16 and 22 on Notice and action mechanisms and Statement of Reasons, Article 25 on Online interface design and organisation, Articles 15 and 24 on Transparency, Article 26 on Advertisements, Article 27 on Recommender systems and Article 44 on Standards.

(10) This includes the following provisions of Regulation (EU) 2022/2065: Articles 34 and 35 on Risk assessment and Mitigation of risks, Article 38 on Recommender systems, Article 40 on Data access and scrutiny and Article 44 (j) on standards for targeted measures to protect minors online.

additional measures which are not set out in these guidelines and which are necessary for them to comply with the obligations stemming from those provisions ([11]).

10. Article 28(1) of Regulation (EU) 2022/2065 should also be seen in the light of other Union legislation and non-binding instruments which aim to address the risks to which minors are exposed online ([12]). Those instruments also contribute to achieving the objective of ensuring a high level of privacy, safety and security of minors online, and thus complement the application of Article 28(1) of Regulation (EU) 2022/2065. These guidelines should not be understood as interpreting or pre-empting any obligations arising under those instruments or under Member State legislation. Oversight and enforcement remain the sole responsibility of the competent authorities designated under those legal frameworks. In particular, as clarified in recital 10 of Regulation (EU) 2022/2065, the present guidelines are without prejudice to other acts of Union law regulating the provision of information society services in general, regulating other aspects of the provision of intermediary services in the internal market or specifying and complementing the harmonised rules set out in Regulation (EU) 2022/2065, such as Directive 2010/13/EU, as well as Union law on consumer protection and on the protection of personal data, in particular Regulation (EU) 2016/679.

11. While these guidelines set out measures that ensure a high level of privacy, safety and security for minors online, providers of online platforms are encouraged to adopt those measures for the purposes of protecting all users, and not just minors. Creating a privacy preserving, safe and secure online environment for all users will inherently result in more privacy, safety and security for minors online.

(11) This includes Articles 34 and 35 on Risk assessment and Mitigation of risks, Article 38 on Recommender systems and Article 40 on Data access and scrutiny.

(12) This approach includes the Better Internet for Kids strategy (BIK+), Directive 2010/13/EU ("the Audiovisual Media Services Directive"), Regulation (EU) 2024/1689 ("the AI Act"), Regulation (EU) 2016/679 ("GDPR"), the Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children, the EU Digital Identity Wallet and the short-term age verification solution, the forthcoming action plan against cyberbullying, the EU-wide inquiry on the broader impacts of social media on well-being, the ProtectEU Strategy, the EU Roadmap to fight drug trafficking and organised crime, the EU Internet Forum, the EU Strategy for a more effective fight against child sexual abuse, the EU Strategy combating trafficking in human beings 2021-2025. Further, Regulation (EU) 2022/2065 is without prejudice to Union law on consumer protection and product safety, including Regulations (EU) 2017/2394 and (EU) 2019/1020 and Directives 2001/95/EC and 2013/11/EU. The Commission also recalls the European Commission Fitness Check of EU consumer law on digital fairness.

12. In accordance with Article 28(4) of Regulation (EU) 2022/2065, the Commission consulted the European Board for Digital Services on a draft of these guidelines prior to their adoption.

13. By adopting these guidelines, the Commission indicates that it will apply these guidelines to the cases described therein and thus that it imposes a limit on the exercise of its discretion whenever applying Article 28(1) of Regulation (EU) 2022/2065. As such, these guidelines may therefore be considered a significant and meaningful benchmark on which the Commission as well as digital services coordinators and competent authorities will base itself when applying Article 28(1) of Regulation (EU) 2022/2065 and determining the compliance of providers of online platforms accessible to minors with that provision. ([13]) Nevertheless, adopting and implementing measures set out in these guidelines, either partially or in full, shall not automatically entail compliance with that provision.

14. The Commission recalls Article 52 of Regulation (EU) 2022/2065 which provides for penalties in the event of infringement of that Regulation.

15. Any authoritative interpretation of Article 28(1) of Regulation (EU) 2022/2065 may only be given by the Court of Justice of the European Union, which amongst others has jurisdiction to give preliminary rulings concerning the validity and interpretation of EU acts, including Article 28(1) of Regulation (EU) 2022/2065.

3 STRUCTURE AND APPLICATION

16. Section 4 of these guidelines sets out the general principles which should govern all measures that providers of online platforms accessible to minors put in place to ensure a high level of privacy, safety, and security of minors on their service. Sections 5 to 8 of these guidelines set out the main measures that the Commission considers that such providers should put in place to ensure such a high level of privacy, safety and

(13) Adopting and implementing any of the measures set out in these guidelines also does not entail compliance of any of such measures with the GDPR or any other applicable data protection law. In determining compliance with article 28(1), responsible authorities are therefore encouraged to cooperate with data protection authorities.

security. These include Risk review (section 5), Service design (section 6), Reporting, user support and tools for guardians (section 7) and Governance (section 8).

17. The measures described in Sections 5 to 8 of these guidelines **are not exhaustive**. Other measures may also be deemed appropriate and proportionate to ensure a high level of privacy, safety and security for minors in accordance with Article 28(1) of Regulation (EU) 2022/2065, such as those measures resulting from compliance with other pieces of EU legislation or adherence to national guidance on the protection of minors ([14]) or technical standards ([15]). In addition, new measures may be identified in the future that enable providers of online platforms accessible to minors to better comply with their obligation to ensure a high level of privacy, safety and security of minors on their service.

4 GENERAL PRINCIPLES

18. The present guidelines are based on the following general principles, which are interrelated and should be considered holistically in all the activities by providers of online platforms that are in scope of these guidelines. The Commission considers that any measure that a provider of an online platform accessible to minors puts in place to comply with Article 28(1) of Regulation (EU) 2022/2065 should adhere to the following general principles.

19. **Proportionality and appropriateness:** Article 28(1) of Regulation (EU) 2022/2065 requires any measure taken to comply with that provision to be appropriate and proportionate to ensure a high level of privacy, safety, and security of minors. Since different online platforms may pose different types of risks for minors, it will not always be proportionate or appropriate for all providers of online platforms to apply all, or only some of the measures described in these guidelines. Determining whether a particular measure is proportionate, in particular where it entails an interference with

(14) This includes for example the Directives and Regulations cited in footnote 12, the forthcoming guidelines by the European Data Protection Board (EDPB) on processing of minor personal data in accordance with Regulation (EU) 2016/679 (GDPR).

(15) CEN-CENELEC (2023) *Workshop Agreement 18016 Age Appropriate Digital Services Framework*; OECD. (2021). *Children in the digital environment - Revised typology of risks*. Available: https://www.oecd.org/en/publications/children-in-the-digital-environment_9b8f222e-en.html.

individuals' fundamental right to data protection, will require a case-by-case review by each provider (i) of the risks to minors' privacy, safety and security stemming from its online platform or parts of it, considering inter alia the size, reach and type of service it provides and its nature, its intended or current use, its specific features and the user base of the service, (ii) of the impact of the measure on children's rights and other rights and freedoms enshrined in the Charter of Fundamental Rights of the European Union ("the Charter"); (iii) the extent to which the measure is appropriate for the purpose of providing a high level of privacy safety and security for minors on their platforms, based on the highest available standards and existing good practices, as well as the perspective and rights of children; and (iv) the suitability of the measure, given the nature of the online platform (see Section 5 on Risk review).

20. **Children's rights:** These rights are enshrined in the Charter and the United Nations Convention on the Rights of the Child ("the UNCRC"), to which all Member States are parties (16). Children's rights form an integral part of human rights, and all those rights are interrelated, interdependent and indivisible. Therefore, to ensure that measures to achieve a high level of privacy, safety and security for minors on an online platform are appropriate and proportionate, all children's rights should be considered and their best interest prioritised, taking into account the diversity of children based on their race, colour, sex, language, religion, political or other opinion, national, ethnic or social origin, property, disability, birth or other status. Children's rights include for instance their right to protection, non-discrimination, inclusion, privacy, access to information and education, freedom of expression as well as to have their views taken into account in all matters that affect them (17).

21. **Privacy-, safety- and security-by-design**: providers of online platforms accessible to minors should integrate the highest standards of privacy, safety and security in the

(16) These rights are elaborated by the United Nations Committee on the Rights of the Child as regards the digital environment in their General Comments No. 25. Office of the High Commissioner for Human Rights. (2021). General Comment No. 25 (2021) on children's rights in relation to the digital environment. Available: https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation.

(17) At this regard, the Commission recalls the importance of accessibility, including as regulated in Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies ("Web Accessibility Directive"), as well as child participation throughout the design, implementation, and evaluation of all safety, security and privacy measures concerning children online.

design, development and operation of their services ([18]). By design concepts aim to harness the influence of providers of online platforms, designers and policymakers to shape product and service development in ways that prioritise values that promote human well-being. They refer to embedding privacy, safety and security protections by default into the design, operation and management of organisations, as well as in products and services from the start ([19]).

22. **Age-appropriate design:** providers of online platforms accessible to minors should design their services to align with the developmental, cognitive, and emotional needs of minors, while ensuring their safety, privacy, and security. Age-appropriate designs are suitable for children considering their rights and well-being as well as their diversity and specific age or stage of development and take account of the evolving capacities of children ([20]).

5 RISK REVIEW

23. The heterogeneous nature of online platforms may require distinct approaches, with certain measures being better suited to some platforms over others. Where a provider of an online platform accessible to minors is deciding how to ensure a high level of safety, privacy and security to minors on their platform, and determining the appropriate and proportionate measures for that purpose, the Commission considers that that provider should, at a minimum, identify and consider:

(18) According to Article 25 GDPR, operators processing minors' personal data must already implement appropriate organisational and technical measures to protect the rights of data subject (data protection by design and default). This obligation is enforced by the competent data protection authorities in line with Article 51 GDPR. See EDPB guidelines 4/2019 on Article 25 Data Protection by Design and by Default. Available: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en.

(19) OECD (2024), *Towards Digital Safety by Design for Children.* Available: https://doi.org/10.1787/c167b650-en.

(20) This requires prioritising features, functionality, content or models that are compatible with children's evolving capacities, as well as taking into consideration socio-cultural differences. Age-appropriate design is crucial for the privacy, safety and security of children: e.g. without age-appropriate information about it, children may be unable to understand, use or enjoy privacy or safety features, settings or other tools. CEN-CENELEC (2023) *Workshop Agreement 18016 Age Appropriate Digital Services Framework*, available https://www.cencenelec.eu/media/CEN-CENELEC/CWAs/ICT/cwa18016_2023.pdf ; Ages and developmental stages available, *inter alia* as Annex to the *Dutch Children's Code*. Available: https://codevoorkinderrechten.nl/wp-content/uploads/2022/02/Code-voor-Kinderrechten-EN.pdf.

a. How likely it is that minors will access its service, notably in view of its nature, purpose, intended use as well as criteria relevant to determine whether the service is accessible to minors.

b. The actual or potential impact on the privacy, safety and security of minors that the online platform may pose or give rise to, based on the 5Cs typology of risks (Annex I). This includes an examination of how different aspects of the platform may give rise to these risks, their likelihood and severity, as well as consideration of their positive impact on children's rights and well-being, taking into consideration the age and evolving capacities of children. For example, aspects such as the purpose of the platform, its design, interface, value proposition, marketing, features, functionalities, number and type of users and uses (actual and expected) may all be relevant.

c. The measures that the provider is already taking to prevent and mitigate these risks.

d. Any additional measures that are identified in the review as appropriate and proportionate to ensure a high level of privacy, safety and security for minors on their service.

e. Why certain measures are deemed appropriate and proportionate.

f. Metrics that allow the provider to monitor over time the effectiveness of the measures they have in place to address certain risks.

g. The potential positive and negative effects on children's or other users' rights of any measure that the provider currently has in place and any additional measures, ensuring that these rights are not disproportionate or unduly restricted and positive effects can be maximised. Children's or other users' rights that may be adversely affected by some measures include, for example, children's rights to participation, privacy, protection of personal data, freedom of expression and information. This is relevant when determining the proportionality of measures.

24. When conducting this review, providers of online platforms accessible to minors should be informed by the best interest of the minor ([21]) and other UNCRC principles ([22]), as well as to other relevant Union guidance on the matter. ([23]) They should include the perspectives of children by seeking their participation, as well as that of guardians, representatives of other potentially impacted groups and other relevant experts and stakeholders.

25. Providers should consider the most up-to-date available information and insight from scientific and academic sources, including by leveraging other relevant assessments conducted by the provider. They should adhere to the precautionary principle when there is reasonable indication that a particular practice, feature or design choice poses risks to children, taking measures to prevent or mitigate that risk until there is evidence that its effects are not harmful to children.

26. Providers should carry out the review periodically, and at least on an annual basis or whenever they make significant changes to the platform's design ([24]) or become aware of other circumstances that affect how the platform's design and operation affect the privacy, safety and security of minors on their online platform. Providers should make the risk review available to the relevant supervisory authorities and publish its outcomes to the extent that these do not include sensitive operational or security-related information, as well as consider submitting it to the review of independent experts or relevant stakeholders.

(21) Article 3 of the UNCRC; Article 24 of the Charter: The right of the child to have his or her best interest assessed and taken as a primary consideration when different interests are being considered, in order to reach a decision on the issue at stake concerning a child, a group of identified or unidentified children or children in general. Best interest determinations, when necessary, should not be conducted by the companies, but based on competent authorities' action. LSE Digital Futures for Children (2024), *The Best interests of the child in the digital environment*. Available: https://www.digital-futures-for-children.net/digitalfutures-assets/digitalfutures-documents/Best-Interests-of-the-Child-FINAL.pdf.

(22) Non-discrimination: Every child has rights regardless of their race, religion, or abilities; Right to life, survival, and development: Children have the inherent right to life, and states must ensure their survival and development. Respect for the views of the child: Children have the right to express their views freely in all matters affecting them, and their opinions must be given due weight.

(23) The Commission recalls in particular the EDPB Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.

(24) Examples of significant changes are the introduction of new features affecting user interaction, modifications to recommender systems, account settings, moderation, reporting or other design features that would appreciably change children's experience on the platform, changes in data collection practices, expansion to new user groups, integration of generative AI tools, or changes related to age assurance measures or their providers.

27. Existing standards and tools to carry out child rights impact assessments can support providers in carrying out this review. These include, for example, the templates, forms and other guidance provided by UNICEF ([25]), the Dutch Ministry of the Interior and Kingdom Relations (BZK), ([26]) or the European standardisation body CEN-CENELEC. ([27]) The Commission may issue additional guidance or tools to support providers in carrying out the review, including through specific tools for child rights impact assessments. Until the publication of this guidance, providers should use existing tools and best practices for these assessments.

28. For providers of VLOPs this risk review can also be carried as part of the general assessment of systemic risks under Article 34 of Regulation (EU) 2022/2065, which will complement and go beyond the risk review pursued in accordance with the present guidelines.

6 SERVICE DESIGN

6.1 Age assurance

6.1.1 Introduction and terminology

29. In recent years, technology has seen fast developments allowing providers of online platforms to assure themselves in more and less accurate, reliable and robust ways of the age of their users. These measures are commonly referred to as "age assurance" ([28]).

(25) UNICEF. (2024). *Children's rights impact assessment: A tool to support the design of AI and digital technology that respects children's rights.* Available: https://www.unicef.org/childrightsandbusiness/workstreams/responsible-technology/D-CRIA; (2021) MO-CRIA: *Child Rights Impact Self-Assessment Tool for Mobile Operators*, Available: https://www.unicef.org/reports/mo-cria-child-rights-impact-self-assessment-tool-mobile-operators

(26) Dutch Ministry of the Interior and Kingdom Relations (BZK). (2024). *Child Rights Impact Assessment (Fillable Form).* Available: https://www.nldigitalgovernment.nl/document/childrens-rights-impact-assessment-fill-in-document/.

(27) See in particular chapter 14 of CEN-CENELEC (2023) *Workshop Agreement 18016 Age Appropriate Digital Services Framework*, Available: https://www.cencenelec.eu/media/CEN-CENELEC/CWAs/ICT/cwa18016_2023.pdf.

(28) European Commission: Directorate-General for Communications Networks, Content and Technology, Center for Law and Digital Technologies (eLaw), LLM, Raiz Shaffique, M. and van der Hof, S. (2024). *Mapping age assurance typologies and requirements – Research report*. Available: https://data.europa.eu/doi/10.2759/455338

30. Age assurance methods can help providers of online platforms that are - in principle - accessible to minors to ensure a high level of privacy, safety and security for minors on their service. For instance, age assurance tools can help providers to enforce access restrictions for users below a certain age, in order to protect minors from accessing age-inappropriate content online, such as gambling or pornography, or from being exposed to other risks such as grooming.

31. Age assurance tools can also help providers to enforce access restrictions that are used to prevent adults accessing certain platforms that are designed for minors, thus reducing the risk of adults posing as minors and/or seeking to harm minors, except for when doing so for legitimate parental, educational, or supervisory purposes.

32. Finally, age assurance tools can be used to underpin the age-appropriate design of the service itself, thereby fostering safer and more child-suitable online spaces. In these instances, the tools can be used to ensure that children only have access to certain content, features or activities that are appropriate for their consumption, taking into account their age and evolving capacities.

33. It is important to distinguish between, on the one hand, the age restriction that limits access to the platform or to parts thereof to users below or above a certain age, and, on the other hand, the measures or tools that are used to enforce this age restriction and to determine the user's age.

34. The most common age assurance measures currently available and applied by online platforms fall into three broad categories: self-declaration, age estimation, and age verification.

    a. **Self-declaration** consists of methods that rely on the individual to supply their age or confirm their age range, either by voluntarily providing their date of birth or age, or by declaring themselves to be above a certain age, typically by clicking on a button online.

b. **Age estimation** consists of methods which allow a provider to establish that a user is likely to be of a certain age, to fall within a certain age range, or to be over or under a certain age ([29]).

c. **Age verification** is a system that relies on physical identifiers or verified sources of identification that provide a high degree of certainty in determining the age of a user.

35. The main difference between age estimation and age verification measures is the level of accuracy. Whereas age verification provides certainty about the age of the user down to the day, age estimation provides an approximation of the user's age. The accuracy of age estimation technologies may vary and improve as technology progresses.

36. For the purposes of the recommendations set out in this Section 6.1, if and when age verification is recommended, providers of online platforms may use age estimation methods if they can prove that such methods are comparable to those of age verification, in respect of the criteria set out in Section 6.1.4.

6.1.2 Determining whether to put in place access restrictions supported by age assurance measures

37. Before deciding whether to put in place any access restrictions based on age, supported by age assurance methods, providers of online platforms otherwise accessible to minors should always conduct an assessment to determine whether such a measure is appropriate to ensure a high level of privacy, safety and security for minors on their service and whether it is proportionate, or whether such a high level may be achieved already by relying on other less far-reaching measures ([30]). In this regard, the Commission is of the view that providers should consider access restrictions based on age, supported by age assurance measures as a complementary tool to measures set out in other sections of these guidelines. In other words, access restrictions and age assurance alone cannot substitute for measures elsewhere in these guidelines.

(29) ibid; CEN-CENELEC. (2023). *Workshop Agreement 18016 Age Appropriate Digital Services Framework*: https://www.cencenelec.eu/media/CEN-CENELEC/CWAs/ICT/cwa18016_2023.pdf.

(30) The review of risks and [UNICEF child rights impact assessment] outlined in Section 5 on Risk review can help providers of online platforms to conduct this assessment.

38. Such an assessment should ensure that any restriction to the exercise of fundamental rights and freedoms of the recipients, especially minors, is proportionate. Consequently, online platforms should make the result of such an assessment publicly available, both if it suggests no access restriction supported by age assurance is required and in the event that such a restriction would be an appropriate and proportionate measure. In the latter case, the assessment should provide information about any age assurance solutions that are identified and their adequacy and effectiveness. It should also include an overview of the performance metrics used to measure this, such as false positive and false negative rates, and accuracy and recall rates

39. 5If access restriction supported by age assurance is assessed as a necessary and proportionate measure participation of children in the design, implementation, and evaluation of these should be foreseen. Online platforms might have only some content, sections or functions that pose a risk to minors or may have parts of their platform where the risk can be mitigated by other measures and parts where it cannot. In these cases, providers of online platforms should assess which content, sections or functions on their platform carry risks for minors and implement access restrictions supported by age assurance methods to reduce these risks for minors in proportionate and appropriate ways.

6.1.3 Determining which age assurance methods to use

6.1.3.1 Age verification

40. In the following circumstances, the Commission considers the use of **age verification** methods an appropriate and proportionate measure to ensure a high level of privacy, safety, and security of minors:

    a. Where applicable Union or national law prescribes a minimum age to access certain products or services offered and/or displayed in any way on the online platform, such as by way of example:

        i. the sale of alcohol, tobacco or nicotine-related products

        ii. access to pornographic content, or prostitution platforms,

        iii. or access to gambling platforms.

b. Where, due to identified risks to minors, the terms and conditions or any other contractual obligations of the service require a user to be 18 years or older to access the service even if there is no formal age requirement established by law.

c. Where national law, in accordance with Union law, prescribes a minimum age to access certain products or services offered and/or displayed in any way on an online platform, including specifically defined categories of online social media services.

d. Any other circumstances in which the provider of an online platform accessible to minors has identified high risks to minors' privacy, safety, or security, including content risks as well as contact risks (e.g., arising from features such as live chat, image/video sharing, anonymous messaging), where these risks cannot be mitigated as effectively by other less intrusive measures as they can by access restrictions supported by age verification. ([31]).

41. In such cases in particular, in order to limit the risk of fragmentation of the Internal Market and the potentially disruptive effect of requiring verification by all users of the online platform service in the relevant Member State, it should be open to providers of on line platforms to prove that they use an age estimation technology, which is comparable to that of age verification technologies in respect of the criteria set out in Section 6.1.4.

6.1.3.2 Age verification technologies

42. Methods that rely on verified and trusted government-issued IDs, without providing the platform with personal data, may constitute an effective age verification method. Member States are currently in the process of providing each of their citizens, residents and businesses an EU Digital Identity Wallet. ([32])

43. The EU Digital Identity wallets provide a safe, reliable, and private means of electronic identification within the Union and maybe used to share only specific information with a service, such as the age of the person.

(31) These risks can be identified via the review of risks set out in Section 5.

(32) As provided for under Section 1 of Chapter II of Regulation (EU) No 910/2014, as amended by Regulation (EU) 2024/1183.

The EU Digital Wallet

Once implemented the EU Digital Identity Wallets will provide a safe, reliable, and private means of digital identification for everyone in the Union. Every Member State is required to provide at least one wallet to all its citizens, residents, and businesses which should allow them to prove who they are, and to safely store, share and sign important digital documents by the end of 2026.

44. To facilitate age verification before the EU Digital Identity Wallet becomes available, the Commission is currently testing an EU age verification solution as a standalone age verification measure that respects the criteria of effectiveness of age assurance solutions outlined in section 6.1.4. Once finalised, the EU age verification solution will aim to provide a valid example and a compliance benchmark for a device-based method of age verification. Prior to finalisation of the EU age verification solution providers of online platforms, which would otherwise be expected to use age verification solutions for their services, are expected to participate in available testing of early versions of the EU age verification solution, as part of their compliance efforts.

EU age verification solution

The EU age verification solution, including an app, will be an easy-to-use age verification method that can be used to prove that a user is 18 or older (18+). The solution will bridge the gap until the EU Digital Identity Wallet is available. This solid privacy-preserving and data minimising solution will aim to set a standard in terms of privacy and user friendliness.

The EU age verification solution provides a compliance benchmark for the accuracy of an age assurance solution while minimising the impact on the rights and freedoms of the recipients.

Users will be able to easily activate the app and receive the proof in several different ways. The proof only confirms if the user is 18 years or older. It does not give the precise age, nor does it include any other information about the user. The user can present the 18+ proof to the online platform in a privacy-preserving way without data flows to the proof provider. In addition, mechanisms will be in place to prevent tracking across providers of online platforms. The use of the app is simple. When requesting access to adult online content, the user presents the 18+ proof via the app to the online platform. Following verification of its validity, the online platform grants the user access. The user's identity and actions are shielded from disclosure throughout the whole process. The trusted proof provider is not informed about which online services the user seeks to access with the 18+ proof. Likewise, 18+ online service providers do not receive the identity of the user requesting access, only a proof that the user is over the age of 18 years.

The EU age verification solution will be also technically capable of providing other attributes, such as liveness tests. In countries where valid methods for attestations of ages below 18 years are supported, the EU age verification solution can also provide for age verification below the age of 18.

45. Providers of online platforms accessible to minors may use other age verification methods to ensure a high level of privacy, safety, and security of minors, provided that they meet the criteria outlined in Section 6.1.4. The EU age verification solution is an example of a method meeting those criteria.

6.1.3.3 Age estimation

46. The Commission considers the use of **age estimation** methods to be an appropriate and proportionate measure to ensure a high level of privacy, safety, and security of minors in the following circumstances:

    a. Where the online platform service's terms and conditions or similar contractual obligations of the service require a user to be above a required minimum age that is lower than 18 to access the service, indicating the provider's assessment of when the online platform is safe and secure for minors to use ([33]) ([34]).

    b. Where the provider of the online platform has identified at least medium risks to minors on their platform as established in its risk review (see Section 5 on Risk Review) ([35]) and those risks cannot be mitigated by less restrictive measures. The Commission considers this will be the case where the risk is not high enough to require access restriction based on age verification but not low enough that it would be appropriate to not have any access restriction or to have access restriction that is not supported by any age assurance methods or is only supported by self-declaration. Self-declaration is not considered to be an appropriate age-assurance measure as further explained below.

47. Providers of online platforms accessible to minors, in particular social media platforms, that meet one or both of the circumstances set out in the paragraphs above, may also put in place the EU age verification solution or other age verification methods to support their access restrictions, provided that these methods meet the criteria outlined in Section 6.1.4.

(33) Where age verification is used in these instances, it would be without prejudice to any separate obligations on the provider, e.g. requiring it to assess whether the minor as a consumer was old enough to legally enter into a contract. This depends on the applicable law of the Member State where the minor is resident.

(34) In some cases, it may be possible for the provider to verify that the minor was signed up by their guardians.

(35) These risks can be identified via the review of risks set out in Section 5.

48. In any event, providers should conduct a proportionality assessment justifying the adoption of age assurance measures that support their access restrictions, prior to putting them in place. It is important to note that a lower accuracy of a solution does not automatically equate to a lower impact on the fundamental rights and freedoms of recipients, as less accurate solutions may process more personal data than more accurate ones. They may also prevent some children from accessing platforms that they may otherwise be able to access due to the lower level of accuracy. When considering age assurance methods that require the processing of personal data, providers of online platforms accessible to minors should take into account the European Data Protection Board (EDPB) statement on Age Assurance ([36]).

Recommended measure	Scenarios
Age verification only	- Union or national law restricted content and goods, such as pornography and gambling platforms - National law, in accordance with Union law, prescribing a minimum age to access certain products or services, such as specifically defined categories of online social media services - Services designed for an adult audience only, posing risks to minors, such as adults dating platforms. - Terms and conditions and/or any other contractual obligations requiring minimum age of 18 - High risk services where only AV would protect minors, as established in the risk review (see Section 5 on Risk Review)
Age estimation or age verification	- Terms and conditions requiring minimum age lower than 18 to access the service, due to identified risks for minors under the indicated age. - Medium risk services - age assurance is used to ensure age-appropriate experiences for minors online

Good practice

MegaBetting ([37]) is an online platform that allows users to bet on the outcome of real-world events. The provider restricts its service to users above 18 years, in line with national law. To ensure that its online platform is not accessible to minors, it relies on the EU age verification solution that only tells the provider whether the user is at least 18 years old. This information is created by a trusted issuer based on the national eID of the user and is received from an

(36) See EDPB statement 1/2025 on Age Assurance. Available: https://www.edpb.europa.eu/system/files/2025-04/edpb_statement_20250211ageassurance_v1-2_en.pdf

(37) All good and poor practice examples in these guidelines refer to fictious online platforms.

application on the user's phone. The provider considers therefore that the system meets the criteria of being highly effective whilst preserving the privacy of the user.

Poor practice

SadMedia is a social media online platform. The provider of SadMedia decided to restrict its services to minors who are at least 13 years old. This was based on its assessment of medium risks that the platform could pose to minors' privacy, safety and security. SadMedia's terms and conditions set out this restriction. To enforce this restriction, the provider of SadMedia relies on an age estimation model that it developed, and that it claims can predict the age of the user with a margin of error of ±2 years. As a result of this margin of error, many minors below the indicated age can access the service and many minors who meet the age require to leave to the user the choice on which method to use are barred from it. SadMedia's age assurance measure is not highly effective and therefore does not ensure a high level of privacy, safety and security for minors on its service.

49. Where a platform has determined that access restrictions supported by age assurance are necessary to achieve a high level of privacy, safety and security for minors on their service, it should offer, where possible, more than one age assurance method, to provide the user with a choice between methods. This will help to avoid the exclusion of users who, despite being eligible to access an online platform, cannot avail themselves of a specific age assurance method. Where age verification or estimation is appropriate and proportionate, for instance when the terms and conditions prescribe a minimum age other than 18 and due to identified risks to minors, a diversity of methods should always be favoured, meaning at least two different age verification or two different estimation methods, or one verification and one estimation method, should be provided ([38]). Where only age verification is appropriate and proportionate as a support measure, at least two age verification methods should be provided. In order to increase effectiveness and user-friendliness, the appropriate age assurance method should be carried out, where possible at account creation, and the age information then used to contribute to an age-appropriate experience on the platform, in addition to other protective measures mentioned in these guidelines. Furthermore,

(38) See also point 17 of the EDPB Statement on age assurance.

providers of online platforms should provide a redress mechanism for users to complain about any incorrect age assessments by the provider ([39]).

Poor practice

SadMedia uses an age estimation solution as one of a range of measures that contribute to a high level of privacy, safety and security. When the age estimation system provides a negative result, indicating that the user is too young to use the service, a pop-up is presented to the user which states "Disagree with the result? Please try again!" The user is then able to redo the age estimation test using the same method. In this example, the age assurance measure would not be considered appropriate or proportionate as no possibility is given to the recipient to use another age assurance method nor is a way of redress provided to the recipient to challenge an incorrect assessment.

6.1.4 Assessing the appropriateness and proportionality of any age assurance method

50. Before considering whether to put in place a specific age verification or estimation method supporting access restrictions, providers of online platforms accessible to minors should consider the following features of that method:

a. **Accuracy.** How accurately any given method determines the age of the user.

The accuracy of an age verification or estimation method should be assessed against appropriate, clear, and publicly available metrics. These metrics are necessary to evaluate the extent to which the method can correctly determine whether a user is above or below a certain age, or a person's age range ([OBJ][40]. Providers of online platforms should periodically review whether the technical accuracy of the method used still matches the state-of-the-art.

b. **Reliability.** How reliable a given method works in practice in real-world circumstances.

For a method to be reliable, it should be available continuously at any time, and work in different real-world circumstances, beyond ideal lab conditions. Providers of online platforms accessible to minors should assess, before

(39) The provider may wish to integrate this mechanism into their internal complaint-handling system under Article 20. See also Section 7.1 of this document.

(40) Inaccurate age assurance may lead to the exclusion of recipients that would be as such eligible to use a service or allow ineligible recipients to access the service despite the age assurance measure in place.

employing a specific age assurance solution, that any data relied upon as part of the age assurance process comes from a reliable source. For example, a self-signed proof of age would not be considered reliable.

c. **Robustness.** How easy it is to circumvent a given method.

A method that is *easy* for minors to circumvent will not be considered robust enough and will therefore not be considered effective. Such level of "easiness" shall be assessed by providers of online platforms accessible to minors on a case-by-case basis, considering the age of the minors to which the specific measures are addressed. Providers of online platforms accessible to minors should also assess whether the age assurance method provides safety and security, in line with the state-of-the-art, to ensure the integrity of the age data being processed.

d. **Non-Intrusiveness.** How intrusive is a given method on users' rights.

Providers of online platforms accessible to minors should assess the impact the chosen method will have on recipients' rights and freedoms, including their right to privacy, data protection and freedom of expression ([41]). According to the European Data Protection Board, and in line with Article 28(3) of regulation 2022/2065 ([42]), a provider should only process the age-related attributes that are strictly necessary for the specific purpose and age assurance should not be used to provide additional means for providers to identify, locate, profile or track natural persons ([43]). If the method is more intrusive than another method that provides the same level of assurance and effectiveness, the less intrusive method should be chosen. This includes an assessment of whether the method provides full transparency about the process in line with Article 12 GDPR and/or puts information about the user at risk.

e. **Non-discrimination.** How a given method can discriminate against some users.

(41) Inappropriate age assurance may create undue risks to recipients' rights to data protection and privacy whereas blanket age assurance could limit access to services beyond what is actually necessary.

(42) See Recital 71 of Regulation (EU) as well 2022/2065 which highlights the need for providers to observe the data minimisation principle provided for in Article 5(1)(c) of Regulation (EU) 2016/679.

(43) See EDPB statement 1/2026 on Age Assurance point 2.3 and 2.4.

Providers of online platform accessible to minors should make sure that the chosen method is appropriate and available for all minors, regardless of disability, language, ethnic, gender, religious and minority backgrounds.

51. Where age assurance measures do not achieve the criteria set out above, they cannot be deemed to be appropriate and proportionate.

52. The Commission considers that **self-declaration** ([44]) does not meet all the requirements above, in particular the requirement for robustness and accuracy. Therefore, it does not consider self-declaration to be an appropriate age assurance method to ensure a high level of privacy, safety, and security of minors in accordance with Article 28(1) of Regulation (EU) 2022/2065.

53. Furthermore, where a third party is used to carry out age verification or estimation, the Commission considers that this should be explained to minors – as in any case - in easy-to-understand language (see section 8.4 on Transparency). In addition, it remains the responsibility of the provider to ensure that the method used by the third party is effective, in line with the considerations set out above. This includes, for example, where the provider intends to rely on solutions provided by operating systems or device operators.

6.2 Registration

54. Registration or authentication may influence whether and how minors are able to access and use a given service in a safe, age-appropriate and rights-preserving way. If it has been determined that age assurance is necessary in order to provide a high level of privacy, safety and security, as well as to provide an age-appropriate experience, registration or authentication can be a first point of use to carry out such process in a proportionate way.

(44)European Commission: Directorate-General for Communications Networks, Content and Technology, Center for Law and Digital Technologies (eLaw), LLM, Raiz Shaffique, M. and van der Hof, S. (2024) *Mapping age assurance typologies and requirements – Research report*. Available: https://data.europa.eu/doi/10.2759/455338;

55. Where registration is not available or required, the provider should assume that any user who does not register has the age of the youngest user allowed by the platform's terms and conditions and should configure their settings accordingly.

56. Where registration is required or offered as a possibility to access an online platform accessible to minors, the Commission considers that the provider of that platform should:

    a. Explain to users the benefits and risks of registration and, where relevant, why registration is necessary (see Section 8.4 on Transparency).

    b. Ensure that the registration process is easy for all minors to access and navigate, according to their evolving capacities, including those with disabilities or additional accessibility needs.

    c. Ensure that the registration process includes measures to help users to understand whether they are old enough to use the service.

    d. Avoid encouraging or enticing users who are below the minimum age required by the online platform accessible to minors to create accounts or to access the service and take measures to reduce the risk of this happening. ([45])

    e. Ensure that it is easy for minors to log out and to have their account, profile and associated data deleted at their request.

    f. Use the registration process as one opportunity to carry out age assurance if necessary, in view of recommendations in Sections 5 and 6.1, as well as highlight the safety features of the platform or service, the rules of conduct along with their respective consequences for violating terms, any identified risks to a minor's privacy, safety or security and resources available to support users.

    g. Ensure that the registration process does not encourage or entice children to make available or share on their profile more information than necessary for the functioning of the service, and that consent from the child's parent or guardian is sought where necessary under Union or Member State law.

(45) This is without prejudice to additional requirements stemming from other laws, such as Article 12 of Regulation (EU) 2016/679.

6.3 Account settings

6.3.1 Default settings

57. Default settings are an important tool that providers of online platforms accessible to minors may use to mitigate risks to minors' privacy, safety and security, such as, for example, the risk of unwanted contact by individuals seeking to harm minors. Evidence suggests that minors tend not to change their default settings, which means that the default settings remain for most users and thus become crucial in driving behaviour ([46]). The Commission therefore considers that providers of online platforms accessible to minors should:

    a. Ensure that privacy, safety and security by design principles are consistently applied to all account settings for minors.

    b. Set accounts for minors to the highest level of privacy, safety and security by default. This includes designing **default settings** in such a way as to ensure safe and age-appropriate settings for minors, taking into account their evolving capacities. These settings should ensure that by default for all minors, as a minimum:

        i. accounts only allow interaction such as likes, tags, comments, direct messages, reposts and mentions by accounts they have previously accepted.

        ii. no account, except the minor's, can download or take screenshots of contact, location or account information, or content uploaded or shared by the minor to the platform.

(46) Willis, L. E. (2014). Why not privacy by default? *Berkeley Technology Law Journal, 29*(1), 61. Available: https://www.btlj.org/data/articles2015/vol29/29_1/29-berkeley-tech-l-j-0061-0134.pdf; Cho, H., Roh, S., & Park, B. (2019). Of promoting networking and protecting privacy: Effects of defaults and regulatory focus on social media users' preference settings. *Computers in Human Behavior, 101*, 1-13. Available: https://doi.org/10.1016/j.chb.2019.07.001.

Examples of features that may put minors' privacy, safety or security at risk include, but are not limited to, enabling location sharing, switching to a public profile, allowing other users to view their contact or follower lists, allowing sharing of media files, and hosting or participating in a live stream.

iii. only accounts that the minor has previously accepted can see their content, posts and account information.

iv. no one can see the minor's activities such as 'liking' content or 'following' another user.

v. geolocation, microphone, photo access and camera, contact synchronisation as well as all not-strictly necessary tracking features are turned off.

vi. the default autoplay of videos and hosting live streams are turned off.

vii. push notifications are turned off by default and are always off during core sleep hours, adapting the core sleep hours to the age of the minor. When push notifications are actively enabled by the user, they should only notify the user about interactions arising from the user's direct contacts and content from accounts or channels that the user actively follows or engages with (for example, push notifications should never be inauthentic and always mentions precisely the user or creator the notification comes from).

viii. features that may contribute to excessive use, such as the number of "likes" or "reactions", "streaks", the "... is typing" function and "read receipts," are turned off.

ix. any functionalities that increase users' agency over their interactions are enabled. This might include, for example, information or friction that slows down content display, posting and user interaction, giving users an opportunity to think before they decide if they want to see more content, or to think before they post.

x. recommendations of other accounts are turned off.

xi. filters that can be associated to negative effects on body image, self-esteem and mental health are turned off.

c. consider whether, depending on children's ages and evolving capacities and the outcome of a provider's risk review, it is necessary to go beyond the minimum standard for default settings set out in this Section 6.3.1 and design default settings that are more restrictive. For example, by designing default settings for

younger minors where, by default, no other user is allowed to engage in certain types of interactions.

d. Regularly test and update default settings, ensuring that they remain effective after all updates, and against emerging online risks and trends, including any risks to minors' privacy, safety and security identified by the provider in the course of their review of risks (see Section 5 on Risk review).

e. Ensure that minors are not in any way encouraged or enticed to change their settings to lower levels of privacy, safety and security, and that any options to change default settings are presented in a neutral way.

f. Ensure that minors are provided with incremental degrees of control over their settings, according to their age, evolving capacities and needs, to support their growing autonomy and provide them with more agency ([47]).

g. Ensure that settings are explained to minors in a child-friendly and accessible way (see Section 6.46.46.46.46.46.4 on Online interface and other tools).

58. Where minors change their default settings or opt into features that put their privacy, safety or security at risk, the Commission considers that the provider of online platform should:

a. Empower minors with the ability to choose between temporarily changing their default settings, for example for a period of time or for current use in that session, and permanently changing their default settings.

b. Enable easy return to default settings, such as a one-click reset or a history-based undo feature for settings that have been changed.

c. Present warning signals at the point at which the minor changes their settings, clearly explaining the potential consequences of their changes.

(47) Minors experience different developmental stages and have different levels of maturity and understanding at different ages. This is recognised *inter alia* in the UN Committee on the Rights of the Child General Comment No. 25 on children's rights in relation to the digital environment 2021, para. 19-21. A practical table on ages and developmental stages is available, inter alia as Annex to the *Dutch Children's Code*. Available at: https://codevoorkinderrechten.nl/wp-content/uploads/2022/02/Code-voor-Kinderrechten-EN.pdf.

d. Periodically provide reminders to minors about the potential consequences of their change and periodically provide them with the opportunity to return to their default settings.

e. Automatically turn off geolocation, microphone and camera as well as not strictly necessary tracking features after the session ends, if a minor turns them on.

f. When geolocation, microphone and camera are switched on, make this obvious to minors throughout the period during which they are switched on.

6.3.2 Availability of settings, features and functionalities

59. The Commission considers that providers of online platforms should:

a. Consider whether some settings, features or functionalities should be removed from minors' accounts altogether and/or whether any of the default settings set out in the previous Section 6.3.1 should be made irreversible or unchangeable for all minors or for minors of certain ages, taking into account their age and evolving capacities. When making this assessment, providers of online platforms accessible to minors should assess the risks that those settings and functionalities may present to the privacy, safety and security of minors on their platform.

b. Ensure that irrespective of the account settings chosen by minors:

i. minors can never be easily found or contacted by accounts they have not previously accepted as contacts.

ii. minors' personal contact details, including email or telephone number, are never disclosed to other users unless explicitly permitted by the minor.

iii. minors' accounts are never included in contact suggestions to adults. Adult accounts or accounts likely to be fake minor accounts are not recommended to minors.

iv. accounts that the minor has not previously accepted as contacts can never see their profile information, biography, activities and history such as 'likes' and 'views', lists of friends and followers and accounts that the minor follows, and that such information always becomes unavailable if the account is blocked or otherwise un-accepted.

c. Ensure that minors are provided with the possibility to restrict the visibility of their profile photo and of individual pieces of content that they publish, as well as the possibility to restrict the visibility of their content generally.

d. Ensure that minors are provided with the possibility to accept or reject any tagging by other users, whether in content, comments or otherwise.

e. Consider how to prevent minors from inadvertently accepting unwanted contacts by, for example, requiring users to include a message when they request to connect with another user.

6.4 Online interface design and other tools

60. The Commission considers that measures allowing minors to take control of their online experiences are an important contribution to ensuring a high level of privacy, safety and security of minors for the purposes Article 28(1) of Regulation (EU) 2022/2065.

61. Without prejudice to the obligations of providers of VLOPs under Section 5 of Chapter III of Regulation (EU) 2022/2065 and independently of the providers of online platforms' obligations as regards the design, organisation and operation of their online interfaces deriving from Article 25 that Regulation, the Commission considers that providers of online platforms accessible to minors should adopt and implement functionalities allowing minors to decide how to engage with their services. These functionalities should provide the right balance between child agency and an adequate level of privacy, safety and security. This should include, for example:

a. Ensuring that online interface design offers an age-appropriate experience for minors.

b. Ensuring that minors are not exposed to persuasive design features that are aimed predominantly at engagement and that may lead to extensive use or overuse of the platform or problematic or compulsive behavioural habits. This includes the possibility to scroll indefinitely, the superfluous requirement to perform a specific action to receive updated information on an application, automatic triggering of video content, notifications artificially timed to regain minors' attention, notifications that are artificial, including those that pretend to be another user or social notifications about content that the user has never engaged with, signs communicating scarcity ([48]), and the creation of virtual rewards for performing (repeated) actions on the platform.

c. Introducing customisable, easy-to access and use, child-friendly and effective time management tools to increase minors' awareness of their time spent on online platforms and to help them engage with the service for no longer than they or their guardians intend. To be effective, these tools should create real frictions so that minors are effectively deterred from spending more time on the platform. These could also include nudges that favour safer options. There should also be systematic implementation of active notifications informing minors of the time spent online.

d. Ensuring that any tools, features, functionalities, settings, prompts, options and reporting, feedback and complaints mechanisms are child-friendly, age-appropriate, easy to find, access, understand and use for all minors, including those with disabilities and/or additional accessibility needs, are engaging, and do not require changing devices to complete any action involved.

e. Ensuring that, if AI features such as AI chatbots and filters are integrated into the service of an online platform, children are not encouraged or enticed to use them, and that such systems are in line with the evolving capacities of children and designed in a way that is safe for children. They should only be available after an assessment of the risks those AI features may pose to children's privacy, safety and security.

(48) The Commission recalls that Directive 2005/29/EC prohibits unfair commercial practices, including in its Annex I, point 7, falsely stating that a product will only be available for a very limited time, or that it will only be available on particular terms for a very limited time, in order to elicit an immediate decision and deprive consumers of sufficient opportunity or time to make an informed choice.

f. Ensure that technical measures are implemented to warn ([49]) minors that interactions with an AI feature are different from human interactions and that these features can provide information that is factually inaccurate and can be misleading. This warning should be easily visible and directly accessible from the interface and throughout the entirety of the minor's interaction with the AI feature. For example, AI chatbots should not be displayed prominently, they should not be part of suggested contacts or grouped with users the minor is connected to. Providers of online platforms should ensure that minors and their guardians have options to opt out of the use of AI chatbots and should not be nudged towards using those features. Such AI features cannot be used to influence or nudge minors towards commercial content or purchases.

Poor practice

SadFriends is a social media platform where minors' profiles are subject to the same settings as adults. Upon sign-up, minors' account information and content are visible to other users on and off the platform. Minors can be contacted by other users who have not been accepted as contacts by the minor. These other users can send them messages and comment on their content. When minors turn on their geolocation to share their location with their friends, their location becomes visible to all accounts they are friends with and remains activated after they close the session, which means that other users can see where they are until the minor remembers to turn off their geolocation.

As a result, malicious actors start targeting minors on SadFriends. Unknown adults reach out to minors and engage with them, building an emotional connection and gaining their trust. Minors are groomed and coerced into creating and sharing child sexual abuse images with their abusers.

6.5 Recommender systems and search features

62. Recommender systems determine the manner in which information is prioritised, optimised and displayed to minors. As a result, such systems have an important impact on whether and to what extent minors encounter certain types of content, contacts or conducts online. Recommender systems may pose and exacerbate risks to

(49) The Commission recalls the obligation for providers of AI systems that are intended to interact directly with natural persons to ensure these are designed and developed in such a way that natural persons concerned are informed they are interacting with an AI system according to Article 50(1) of Regulation (EU) 2024/1689 ("the AI Act"). Any measure taken upon this recommendation should be understood according to and without prejudice with the measures taken to comply with Article 50(1) of the AI Act, including its own supervisory and enforcement regime.

minors' privacy, safety and security online by, for example, amplifying content that can have a negative impact on minors' safety and security ([50]).

63. For the purpose of this section, and in alignment with Article 3(s) of Regulation (EU) 2022/2065, recommender systems include systems deployed for content recommendations, product recommendations, advertisement recommendations, contact recommendation, search autocomplete and results.

64. The Commission recalls the obligations for all providers of all categories of online platform concerning recommender system transparency under Article 27 of Regulation (EU) 2022/2065 and the additional requirements for providers of VLOPs and VLOSEs under Articles 34 (1), 35(1), and 38 of Regulation (EU) 2022/2065 in this respect ([51]).

65. In order to ensure a high level of privacy, safety and security specifically for minors as required under Article 28 (1) of Regulation (EU) 2022/2065, the Commission considers that providers of online platforms accessible to minors should put in place the following measures:

6.5.1 Testing and adaptation of the design and functioning of recommender systems for minors

66. Providers of online platforms accessible to minors that use recommender systems in the provision of their service should:

(50) Munn, L. (2020). Angry by design: Toxic communication and technical architectures. *Humanities and Social Sciences Communications, 7*(53). Available: https://doi.org/10.1057/s41599-020-00550-7; Milli, S. et al. (2025). Engagement, user satisfaction, and the amplification of divisive content on social media. *PNAS Nexus*, 4(3) pgaf062. Available: https://doi.org/10.1093/pnasnexus/pgaf062; Piccardi, T. et al. (2024). Social Media Algorithms Can Shape Affective Polarization via Exposure to Antidemocratic Attitudes and Partisan Animosity. Available: 10.48550/arXiv.2411.14652; Harriger, J. A., Evans, J. L., Thompson, J. K., & Tylka, T. L. (2022). The dangers of the rabbit hole: Reflections on social media as a portal into a distorted world of edited bodies and eating disorder risk and the role of algorithms. *Body Image, 41*, 292-297. Available: https://doi.org/10.1016/j.bodyim.2022.03.007; Amnesty International. (2023). *Driven into darkness: How TikTok's 'For You' feed encourages self-harm and suicidal ideation*. Available: https://www.amnesty.org/en/documents/pol40/7350/2023/en/; Hilbert, M., Ahmed, S., Cho, J., & Chen, Y. (2024). *#BigTech @Minors: Social media algorithms quickly personalize minors' content, lacking equally quick protection*. Available: http://dx.doi.org/10.2139/ssrn.4674573.

(51) The Commission also recalls that other Union or national law may impact the design and functioning of recommender systems, with a view to ensure protection of legal interests within their remits, which contribute to a high level of privacy, safety and protection of fundamental rights online.

a. Regularly test and adapt their recommender systems to enhance the privacy, safety and security of minors and in accordance with the risk review provided under Section 5, which includes a consideration of children's broader rights. Such testing and adaptation should be conducted by consulting children, guardians and independent experts.

b. Take into account specific needs, characteristics, disabilities and additional accessibility needs of minors, also with due consideration to their age group, when defining the objectives, parameters and evaluation strategies of recommender systems. Parameters and metrics related to accuracy, diversity, inclusivity and fairness should be prioritized,

c. Ensure that recommender systems do not exclusively rely on the collection of behavioural data that captures all or most of the minor's activities on the platform, such as watch time and click through rates.

d. Recommender systems should rely on "implicit engagement-based signals" only in the best interest of the minor and within the specific purpose of enhancing their safety and security, provided that such use is clearly defined and subject to appropriate safeguards as further defined in the recommendations above. For the purposes of the present guidelines, 'implicit engagement-based signals' shall be understood as referring to signals and data that infer user preferences from their activities (browsing behaviour on a platform), such as time spent viewing content and click-through rates.

e. Recommender systems should not rely on the collection of any behavioural data that captures the user's activities off the platform.

f. Prioritise 'explicit user-provided signals' to determine the content displayed and recommended to minors. The selection of such signals should be justified in the best interest of the minor [EDPB: taking into account the principle of data minimisation and transparency], which will help to ensure that they contribute to a high level of safety and security for minors. For the purposes of the present guidelines, 'explicit user-provided signals' shall be understood as referring to user feedback and interactions that indicate users' explicit preferences, both

positive and negative, including the stated and deliberative selection of topics of interest, surveys, reporting ([52]), and other quality-based signals.

g. Implement measures to prevent and reduce a minor's exposure to content recommendations that could pose a risk to their safety and security, particularly when encountered repeatedly, such as content promoting unrealistic beauty standards or dieting, content that glorifies or trivialises mental health issues, such as anxiety or depression, discriminatory content, radicalisation content and distressing content depicting violence or encouraging minors to engage in dangerous activities. This includes content that has been reported or flagged by users, trusted flaggers or other actors or content moderation tools, and whose lawfulness and adherence to the platform's terms and conditions have not yet been verified. This recommendation should be without prejudice to the obligations related to illegal content moderation contained in Regulation (EU) 2022/2065 and to Section 6.7 of this guidelines.

h. Implement measures to ensure that recommender systems do not enable or facilitate the dissemination of illegal content or the commitment of criminal offences against and by minors.

i. Ensure that minors' search results and suggestions for contacts prioritise accounts whose identity has been verified and contacts connected to the network of the minor, or contacts in the same age range as the minor.

j. Ensure that search features, including but not limited to text autocomplete on the search bar and suggested terms and key phrases, do not recommend content that is illegal and/or qualifies as harmful to the privacy, safety or security of minors, for instance by blocking search terms that are well-known to trigger content that is deemed to be harmful to minors' privacy, safety and/or security, such as particular words, slang, hashtags or emojis ([53]). Upon queries related to such

(52) For example, minors' feedback about content, activities, individuals, accounts or groups that make them feel uncomfortable or that they want to see more or less of should be taken into account in the ranking of the recommender systems. This includes feedback such as "Show me less/more", "I don't want to see/I am not interested in", "I don't want to see content from this account," "This makes me feel uncomfortable," "Hide this," "I don't like this," or "This is not for me." See also section 7.1 on user reporting, feedback and complaints of the present guidelines.

(53) Examples of terms can be found in the Knowledge Package on Combating Drug Sales Online, which was developed as part of the EU Internet Forum and compiles more than 3 500 terms, emojis and slangs

content, providers of online platforms should redirect minors to appropriate support resources and helplines.

6.5.2 User control and empowerment

67. Providers of online platforms accessible to minors that use recommender systems, in the provision of their service should adopt the following measures to ensure a high level of privacy, safety and security of minors:

    a. Provide minors with the opportunity to reset their recommended feeds completely and permanently.

    b. Within the prioritization of parameters and metrics related to accuracy, diversity, inclusivity and fairness, provide information and nudge minors toward searching for new content after a certain amount of interaction with the recommender system.

    c. Ensure that minors can choose an option of their recommender system that is not based on profiling and assess whether this should be provided as a default setting depending on the beneficial impact on the safety, privacy and security of the minor.

    d. Ensure that relevant reporting and feedback mechanisms set out in Section 7.1 have a swift, direct and lasting impact on the parameters, editing and output of the recommender systems. This includes permanently removing reported content and contacts from recommendations (including content reported for hiding and blocked/reported contacts) and reducing the visibility of similar content and accounts.

68. In addition to the obligations set out in Article 27(1) of Regulation (EU) 2022/2065, providers of online platforms accessible to minors should put in place the following measures:

    a. Ensure that any settings and information provided to minors about their recommender systems, including but not limited to their Terms and Conditions, are presented in child-friendly and accessible ways (see Sections 6.4 on Online

used by drug traffickers to sell drugs online - see reference in the EU Roadmap to fight against drug trafficking and organised crime, COM/2023/641 final.

interface design and other tools and Section 8.4 on Transparency for more details).

b. Meaningfully explain why each specific piece of content was recommended to them, including information about the parameters used and the user signals collected for that specific recommendation.

c. Offer minors the options to modify or influence the parameters of their recommender systems by, for example, allowing them to select content categories and activities they are most or least interested in. This should be offered during the account creation process and regularly throughout the user's time on the platform. These preferences should directly influence the recommendations provided by the system, ensuring that they align more closely with the minor's age and best interests ([54]). These user control options should be provided in an accessible way and tailored to child-friendly language and design.

6.6 Commercial practices

69. Minors are particularly exposed to the persuasive effects of commercial practices and have a right to be protected against economically exploitative practices ([55]) by online platforms. They are confronted with commercial practices by online platforms, facing diverse, dynamic and personalised persuasive tactics through, for example, advertisement, product placements, the use of in-app currencies, influencer marketing, sponsorship or AI-enhanced nudging ([56]). This can have a negative effect on minors' privacy, safety and security when using the services of an online platform.

(54) See Articles 27(1) and (3) of Regulation (EU) 2022/2065.

(55) UN Committee on the Rights of the Child General Comment No. 25, para 112; UNICEF. (2019). Discussion paper: Digital marketing and children's rights. Available: https://www.unicef.org/childrightsandbusiness/media/256/file/Discussion-Paper-Digital-Marketing.pdf.

(56) This makes it difficult for them, for instance, to distinguish between commercial and non-commercial content, to resist peer pressure to buy in-game or in-app content that are attractive for minors or even necessary to progress in the game, or to understand the real currency value of in-app currencies or that the occurrence of the most desirable content such as upgrades, maps and avatars may be less frequent in randomised in-app or in-game purchases than less desirable content. M. Ganapini, E. Panai (2023) *An Audit Framework for Adopting AI-Nudging on Children*. Available: https://arxiv.org/pdf/2304.14338.

70. In line with, and without prejudice to, the existing horizontal legal framework, in particular the Unfair Commercial Practices Directive 2005/29/EC that is fully applicable to all commercial practices also towards minors ([57]) and the more specific rules in Regulation (EU) 2022/2065 on advertising (Articles 26 and 28(2)) and dark patterns (Article 25), the Commission considers that providers of online platforms accessible to minors should adopt the following measures to ensure a high level of privacy, safety, and security of minors, on their service for the purposes Article 28(1) of Regulation (EU) 2022/2065:

    a. Ensure that minors' lack of commercial literacy is not exploited by considering minors' age, vulnerabilities and limited capacity to engage critically with commercial practices on the platform and provide relevant support ([58]).

    b. Have a responsible marketing and advertising policy in place that does not allow harmful, unethical and unlawful advertising ([59]) to, for or by minors. This entails considering the appropriateness of advertising campaigns for different age groups, addressing their adverse impact, and taking adequate security measures to protect minors as well as to ensure that they have access to information that is in their best interest ([60]).

(57) The Commission recalls that per its Article 2(4) Regulation (EU) 2022/2065, it is without prejudice to Directive 2010/13/EU, Union law on copyright and related rights, Regulation (EU) 2021/784, Regulation (EU) 2019/1148, Regulation (EU) 2019/1150, Union law on consumer protection (including Regulation (EU) 2005/29 and product safety, Union law on the protection of personal data, Union law in the field of judicial cooperation in civil matters, Union law in the field of judicial cooperation in criminal matters and a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings. Further, it shall not affect the application of Directive 2000/31/EC. Under Article 91 of Regulation (EU) 2022/2065, the Commission is mandated to evaluate and report, by 17th November 2025, on the way that this Regulation interacts with other legal acts, in particular the acts referred to above.

(58) UNICEF provides resources and guidance for platforms related to digital marketing ecosystem, including UNICEF (2025) *Discussion Paper on digital marketing and children's rights* Available https://www.unicef.org/childrightsandbusiness/workstreams/responsible-technology/digital-marketing.

(59) For instance, traders are subject to the prohibition under Directive 2005/29/EC Article 5(1) to commit unfair commercial practices and point 28 of Annex I of the Directive prohibits direct exhortation to children to buy advertised products or persuade their parents or other adults to do so. This commercial behaviour is in all circumstances considered unfair.

(60) Committee on the Rights of the Child's General comment No. 25 (2021) on children's rights in relation to the digital environment provides that the best interests of the child should be "a primary consideration when regulating advertising and marketing addressed to and accessible to children. Sponsorship, product placement and all other forms of commercially driven content should be clearly distinguished from all other content and should not perpetuate gender or racial stereotypes."

c. Enforce the marketing and advertising policy efficiently and regularly review the policy in consultation with minors, guardians and other relevant stakeholders.

d. Ensure that minors are not exposed to excessive total volumes, frequency and recommendation of commercial content, that can lead to excessive or unwanted spending or addictive behaviours and have detrimental effects on their privacy, safety and security.

e. Ensure that if AI systems are integrated in the platform, these do not influence or nudge children for commercial purposes, particularly through conversational or advisory formats such as chatbots ([61]).

f. Ensure that declarations of commercial communication are clearly visible, child-friendly, age-appropriate and accessible (see Section 8.4 on Transparency) and consistently used throughout the service, for instance with the use of an icon or a similar sign to clearly indicate that content is advertising. These should be regularly tested and reviewed in consultation with minors, their guardians and other relevant stakeholders.

g. Ensure that minors are not exposed to marketing and communication of products or services that can have an adverse impact on their privacy, safety and security, including as identified in the provider's risk review, including those associated with negative impacts on their physical and mental health (see Section 5 on Risk review).

h. Seek to ensure that minors are not exposed to hidden or disguised advertising, whether placed by the provider of the online platform or the users of the service ([62]). In this context, the Commission recalls that providers of online platforms

(61) The Commission recalls that such AI systems could constitute prohibited practices under Article 5(1)(b) of Regulation (EU) 2024/1689, if they exploit vulnerabilities of children in a manner that causes or is reasonably likely to cause significant harm. Any measures taken according to this recommendation should go beyond measures taken to prevent the application of that prohibition. The supervision and enforcement of measures taken to comply with Article 50(1) of Regulation (EU) 2024/1689 remains the responsibility of the competent authorities under that Regulation.

(62) The Commission recalls that Directive 2005/29/EC Article 7(2), and in Annex I, point 22, prohibits falsely claiming or creating the impression that the trader is not acting for purposes relating to his trade, business, craft or profession, or falsely representing oneself as a consumer. It also recalls Directive 2010/13/EU that prohibits to directly exhort minors to buy or hire a product or service, encourage them to persuade their parents or others to purchase the goods or services being advertised, exploit the special trust minors place in parents, teachers or other persons. According to recital 10 of Regulation 2022/2065

are also obliged, under Article 26(2) of Regulation (EU) 2022/2065, to provide recipients of the service with a functionality to declare whether the content they provide is or contains commercial communications ([63]). Examples of disguised commercial communications may include, but are not limited to, product placements by influencers, product showcases and other forms of subtle promotion that may deceive or manipulate minors into purchasing products or services.

i. Ensure transparency of economic transactions in an age-appropriate way, including in accordance with the requirements of consumer protection legislation, and ensure that children are not exposed to techniques which can have the effect of reducing transparency of economic transactions and may be misleading for minors, such as certain intermediate virtual currencies, ([64]) like tokens or coins, that can be exchanged with real money and used to purchase virtual items, thus also cause unwanted spending.

j. Ensure that minors, when accessing online platforms or parts and features thereof that are presented or appear as being free ([65]), are not exposed to in-app or in-game purchases that are or appear to be necessary to access or use the service. If minors are exposed to any other in app or in-game purchases, they should always be priced in the national currency.

k. Ensure that minors are not exposed to practices that can lead to excessive or unwanted spending or addictive behaviours, by ensuring that minors are not exposed to virtual items such as paid loot boxes, other products, where they offer random or unpredictable outcomes or gambling-like features, and by introducing separation or friction between content and the purchasing of related products.

---

the Regulation should be without prejudice to Union law on consumer protection including Directive 2005/29 concerning unfair business-to-consumer commercial practices in the internal market.

(63) The Commission also recalls that Directive 2010/13/EU provides that video sharing platforms need to have a functionality to declare that content uploaded contains audiovisual commercial communications.

(64) The Commission recalls that the concept of virtual currency is defined in virtual currency is defined in Directive (EU) 2018/843 on anti-money-laundering.

(65) The Commission recalls that Directive 2005/29/EC in its Annex I, point 20, prohibits describing a product as ‘gratis’, ‘free’, ‘without charge’ or similar if the consumer has to pay anything other than the unavoidable cost of responding to the commercial practice and collecting or paying for delivery of the item.

l. Ensure that minors are not exposed to manipulative design techniques ([66]), such as scarcity ([67]), intermittent or random rewards, or persuasive design techniques ([68]) that can lead to excessive or unwanted spending or addictive behaviours.

m. Ensure that minors are not exposed to unwanted purchases, e.g. by considering deploying effective tools for guardians or submitting any financial commitment made by minors under a certain age to the review or consent of guardians (see Section 7.3 on Tools for guardians).

n. Review the platform's ability and opportunity to offer economic transactions, based on the evolving capacities of children, considering that certain age groups should not be exposed or allowed to enter into economic transactions as they do not yet possess the ability to comprehend spending and money.

6.7 Moderation

71. Moderation can reduce minors' exposure to content and behaviour that is harmful to their privacy, safety and security, including illegal content or content that may impair their physical or mental development, and it can contribute to crime prevention.

72. The Commission recalls the obligations related to: terms and conditions set out in Article 14 of Regulation (EU) 2022/2065; transparency reporting provided in Article 15 of that Regulation for providers of intermediary services, which includes providers of online platforms; notice and action mechanisms and statements of reasons provided respectively in Article 16 and 17 of that Regulation for providers of hosting services,

(66) As set out in Article 25 of Regulation (EU) 2022/2065.

(67) The Commission recalls that Directive 2005/29/EC in its Annex I, point 7, prohibits falsely stating that a product will only be available for a very limited time, or that it will only be available on particular terms for a very limited time, in order to elicit an immediate decision and deprive consumers of sufficient opportunity or time to make an informed choice. Thereby traders are subject to the prohibition to use scarcity techniques including scarcity techniques

(68) The Commission recalls that, in the case of games, under Articles 8 and 9 of Directive 2005/29/EC traders should not exploit behavioural biases or introduce manipulative elements relating to, e.g. the timing of offers within the gameplay (offering micro-transactions during critical moments in the game), the use of visual and acoustic effects to put undue pressure on the player.

including online platforms; the obligations related to trusted flaggers ([69]) for providers of online platforms set out in Article 22 of that Regulation. It also recalls the 2025 Code of Conduct on Countering Illegal Hate Speech Online+ and the Code of Conduct on Disinformation which constitute Codes of Conduct within the meaning of Article 45 of Regulation (EU) 2022/2065.

73. In addition to those obligations, the Commission considers that providers of online platforms accessible to minors should put in place the following measures to ensure a high level of privacy, safety, and security of minors on their service for the purposes Article 28(1) of Regulation (EU) 2022/2065:

    a. Define clearly and transparently what the platform considers as content and behaviour that is harmful for minors' privacy, safety and security, in cooperation with minors, civil society and independent experts, including academia. This should include any content and behaviour that is illegal under EU or national law. Providers of online platforms accessible to minors should communicate information concerning their standards and expectations regarding content and behaviour clearly to minors using their service and this information should be available during the set-up of an account and easy to locate on the platform.

    b. Establish moderation policies and procedures that set out how content and behaviour that is harmful for the privacy, safety and security of minors is detected and how it will be moderated aiming at limiting minors' exposure to harmful content. Providers of online platforms should also ensure that these policies and/or procedures are enforced in practice.

    c. Assess and review policies and procedures to ensure that they remain effective as technologies and online behaviours change. Take into account the following factors when prioritising moderation: the likelihood and seriousness of the content causing harm to a minor's privacy, safety and/or security, the impact of

(69) Trusted flaggers are entities with particular expertise and competence in detecting certain types of illegal content, and the notices they submit within their designated area of expertise must be given priority and processed by providers of online platforms without undue delay. The trusted flagger status is awarded by the Digital Services Coordinator of the Member State where the entity is established, provided that the entity has demonstrated their expertise, competence, independence from online platforms, as well as diligence, accuracy and objectivity in submitting notices.

the harm on that minor, specific vulnerabilities and the number of minors who may be harmed. Additionally, reports made by minors should be prioritised.

d. Ensure human review for any reported accounts or content that the provider suspects may pose a risk of harm to minors' privacy, safety or security.

e. Ensure that content moderation teams are well-trained and resourced and that moderation mechanisms are active and functioning at all times (24 hours a day, 7 days a week) to deliver effective moderation, including at least one employee who is on call to respond to urgent requests and emergencies at all times.

f. Ensure that content moderation systems and practices are available and operational in the official language(s) of the Member State the service is provided in.

g. Put in place effective technologies, internal mechanisms and preventative measures to reduce the risk of content and behaviour that are harmful to minors' privacy, safety or security from being recommended to minors, including by implementing effective technical solutions to tackle known harmful and illegal content, such as hash matching and URL detection. Providers should also explore potential added benefits of emerging technical solutions such as AI classifiers to detect new or altered content and conduct.

h. Implementing technical solutions to prevent the AI systems on their platform from allowing users to access, generate and disseminate content that is harmful for the privacy, safety and/or security of minors.

    i. Integrating into any AI systems safeguards that detect and prevent prompts that the provider has identified in their moderation policies as being harmful to minors' privacy, safety and/or security. This may include, for example, the use of prompt classifiers, content moderation and other filters.

    ii. Cooperating with other providers of online platforms and relevant stakeholders for the purpose of detecting policy-violating and illegal content and preventing cross-platform dissemination and conduct.

iii. Where a provider of an online platform accessible to minors hosts financial transactions, it should provide a specific channel for reporting fraud and suspicious financial transactions.

74. Providers of online platforms accessible to minors are encouraged to share metrics on content moderation, for example how often they receive user reports, how often they proactively detect content and conduct violations, the types of content and conduct being reported and detected and how the platform responded to these issues.

75. None of the above measures impose a general obligation to monitor content which providers of online platforms accessible to minors either transmit or store. ([70])

Poor practice

SadShare is a social media platform that allows users to upload and share visual content with others. The platform's policies do not include robust content moderation mechanisms to detect and prevent the upload of harmful and explicit content, including child sexual abuse material. This lack of moderation therefore exposes minors to illegal content, and it makes it possible for malicious users to (re-)use existing images. This in turn fuels the demand for child sexual abuse material that inadvertently induces other users to abuse and harm minors to create new material.

7 REPORTING, USER SUPPORT AND TOOLS FOR GUARDIANS

7.1 User reporting, feedback and complaints

76. Effective and child-friendly user reporting, feedback and complaint tools enable minors to express and address features of online platforms that may negatively affect the level of their privacy, safety and security.

77. The Commission recalls the obligations laid down in Regulation (EU) 2022/2065, including the obligations to put in place a notice and action mechanisms in Article 16, to provide a statement of reasons in Article 17, to notify suspicions of criminal offence in Article 18, to put in place an internal complaint handling system in Article 20 and out of court dispute settlement in Article 21, as well as the rules on trusted flaggers in Article 22.

78. In addition to those obligations, the Commission considers that providers of online platforms accessible to minors should put in place the following measures to ensure

(70) See Article 8(1) of Regulation 2022/2065

a high level of privacy, safety, and security of minors on their service for the purposes Article 28(1) of Regulation (EU) 2022/2065:

a. Implement reporting, feedback and complaints mechanisms that:

   i. Are effective, child-friendly and accessible (see Section 6.4 on Online interface design and other tools and section 4 on General principles).

   ii. Allow minors to report content, activities, individuals, accounts, or groups they believe may violate the platform's terms and conditions. This includes any content, user or activity that is considered by the platform to be harmful to minors' privacy, safety, and/or security (see Section 5 on Risk review and Section 6.7 on Moderation).

   iii. Allow all users to report content, activities, individuals, accounts, or groups that they deem inappropriate or undesirable for minors, or where they are uncomfortable with the idea of such content, activities, individuals accounts or groups being accessible to minors.

   iv. Allow all users to report a suspected underage account, where a minimum age is stated in the platform's terms and conditions.

   v. Allow minors to provide feedback about all content, activities, individuals, accounts or groups that they are shown on their accounts and that make them feel uncomfortable or that they want to see more or less of. These options could include phrases such as "Show me less/more", "I don't want to see/I am not interested in", "I don't want to see content from this account," "This makes me feel uncomfortable," "Hide this," "I don't like this," or "This is not for me". Providers of online platforms should ensure that these options are designed in such a way that they are only visible to the user, so that they cannot be misused by others to bully or harass minors on the platform. Providers of online platforms should adapt their recommender systems in response to this feedback (See section 6.5.2 on User control and empowerment) ([71]).

(71) See section 6.5 of the present guidelines for information about how this information should affect the provider's recommender systems.

vi. Where the provider uses age assurance methods, allow any user to access an effective internal complaint-handling system that enables them to lodge complaints, electronically and free of charge, against an assessment by the provider of the user's age. This complaint handling system should fulfil the conditions set out in Article 20 of Regulation (EU) 2022/2065.

b. Ensure that the reporting, feedback and complaints mechanisms established under Article 20 of Regulation (EU) 2022/2065 ([72]):

i. Contribute to a high level of privacy, safety and security for minors.

ii. Are aligned with fundamental rights, in particular children's rights.

iii. Are available for intuitive and immediate access for all minors, including for those with disabilities and/or additional accessibility needs.

iv. Are easy for minors to use and understand, are age-appropriate and engaging (see Section 6.4 on Online interface design and other tools and section 4 on General principles).

v. Are available for non-registered users if they may access the online platform's content.

c. Ensure the availability of an option that allows minors to provide their own reasons for a report or complaint. Providers should avoid reporting categories, but if they are used, ensure that they are adapted to the youngest users allowed on the platform.

d. Ensure that reporting, feedback and complaints are confidential by default, while providing the option for minors to remove anonymity. If anonymity is removed,

(72) Any reference in the remainder of this section to 'complaint' or 'complaints' includes any complaints that are brought against the provider's assessment of the user's age and any complaints that are brought against the decisions referred to in Article 20 of Regulation (EU) 2022/2065. Article 20 of Regulation (EU) 2022/2065 requires providers of online platforms to provide recipients of the service with access to an effective internal complaint-handling system against four types of decisions taken by the provider of the online platform. These are (a) decisions whether or not to remove or disable access to or restrict visibility of the information; (b) decisions whether or not to suspend or terminate the provision of the service, in whole or in part, to the recipients; (c) decisions whether or not to suspend or terminate the recipients' account; and (d) decisions whether or not to suspend, terminate or otherwise restrict the ability to monetise information provided by the recipients.

the provider, should explain to minors when, how and what information related to reports and/or complaints they share with other users or third parties.

e. Prioritise reports that concerns the privacy, safety and security of minors. Providers of online platforms should provide an option to indicate if the minor thinks a report/compliant is urgent, especially when there is an indication of an ongoing privacy, safety or security issue. Response times should be appropriate to the issue being reported or complained about.

f. Provide each minor that submits a report or complaint with a confirmation of receipt of the report or complaint without undue delay. Minors should also receive an age-appropriate explanation of the process that will be followed when reviewing the report or complaint and an explanation of any actions or non-actions taken. The information should include an indicative timeframe for deciding the report or complaint and possible outcomes. Providers of online platforms are encouraged to provide a mechanism for tracking progress and communicating with the platforms.

g. Regularly review the reports, feedback and complaints that they receive. They should use this information to identify and address any aspects of their platform that may compromise the privacy, safety and/or security of minors, refine their recommender systems and moderation practices, improve overall safety standards, and foster a more trustworthy and responsible online environment. These actions should be documented to be reviewable.

h. Cross-platform collaboration should include risk detection, design standards, and research collaboration with trusted actors.

Poor practice

SadLearn is a popular online platform designed for users between 6 and 18 years old. It offers a range of educational and entertaining content. To flag content that is against the terms and conditions of SadLearn, the user must click through four different links. Once the user arrives in the complaints section, they must choose among 15 different complaints categories making it difficult for minors to identify and select the right category. There is no free-text category. If users manage to submit complaints, they do not receive any confirmation or explanation of what will happen next. Moreover, the reporting tool is only available in English and the language is adapted to an adult audience.

7.2 User support measures

79. Putting in place features on online platforms accessible to minors to assist minors to navigate their services and seek support where needed are an effective means to ensure a high level of privacy, safety and security for minors. The Commission therefore considers that providers of online platforms accessible to minors should:

a. Have clear, easily identifiable and accessible support tools that allow minors to seek help when encountering suspicious, illegal or inappropriate content, accounts or behaviour that make them feel uncomfortable. This includes providing block and mute buttons. The support tools should be child-friendly, clearly visible, immediately accessible (see Section 6.4 on Online interface and other tools) and should connect minors directly with the most appropriate support services for their location and age, such as those that form part of the national Safer Internet Centres, INHOPE networks and national child helplines.

b. Limit the use of support tools based on AI, which should not be used as the main tool to interact with children.

c. Introduce directly visible warning messages, links to relevant national support lines ([73]) and other authoritative sources when minors search for, upload, generate, share and receive content that is potentially illegal or harmful for the privacy, safety and security of minors (as explained in the section 6.7 on Moderation). Providers of online platforms should also refer minors to relevant national support lines when a minor submits a report related to such content. The referral should be made immediately after the provider of the online platform becomes aware of the activity or the minor submits a report.

d. If the online platform features functionalities related to user connection, posting content or user communication, provide minors with the option to anonymously block or mute any other user or account, including those that are not connected to them. The block systems should be easy to find and accessible. No information

(73) Such as those that form part of the national Safer Internet Centres and INHOPE networks or other national child helplines such as https://childhelplineinternational.org/.

about the user or their account should be available to any accounts that the user has blocked.

e. If the online platform enables comments on content, provide minors with the option to restrict the types of users who can comment on their content and content about them and/or prevent other users from commenting on their content and content about them, both at the time of posting and thereafter, even if the possibility to comment is restricted to accounts previously accepted as contacts by the minor (as recommended in Section 6.3 on Account settings),

f. If the online platform offers group functions, ensure that minors join a group only after being notified of the invitation and upon accepting that they wish to be part of that group.

Good practice

NiceSpace is a social media platform for users above 13. When users sign up, they are presented with an interactive tutorial "SafeSpace 101" which explains the platform's privacy, safety and security features, including blocking and muting options, comment control and group invitations. NiceSpace also features a prominent "Help" button, connecting the users directly with their local Safer Internet Centre helpline. When searching for potentially harmful content, NiceSpace warns users with contextual prompts and redirects them to safer resources. All information is adapted to the youngest user of the platform.

7.3 Tools for guardians

80. Tools for guardians are software, features, functionalities, or applications designed to help guardians accompany their minor's online activity, privacy, safety and well-being, while respecting children's agency and privacy.

81. The Commission considers that tools for guardians should be treated as complementary to safety by design and default measures and to any other measures put in place to comply with Article 28(1) of Regulation (EU) 2022/2065, including those described in these guidelines. Minors' right to a high level of privacy, safety and security on online platforms must never depend on tools for guardians. Tools for guardians should not be used as the sole measure to ensure a high level of privacy, safety and security of minors on online platforms, nor be used to *replace* any other

measures put in place for that purpose. Nevertheless, the Commission notes that, when used in combination with other measures, they may contribute to such a high level.

82. Therefore, the Commission considers that providers of online platforms accessible to minors should put in place guardian control tools for the purposes Article 28(1) of Regulation (EU) 2022/2065 which should:

a. Be age-appropriate and in line with the evolving capacities of minors. Tools for guardians should be grounded in communication, learning and empowerment rather than control and enable autonomy and agency of minors. They should be effective and not disproportionately restrict minors' rights to privacy or access services, considering the best interest of the minor.

b. Be easy to use, access and activate for example by allowing the guardian to use the tool without creating an account on the service.

c. Apply regardless of the device or operating system used to access the service.

d. Provide a clear notification to minors of their activation by guardians and put other safeguards in place considering their potential misuse by guardians such as, for example, providing a clear sign to the minor in real time when any monitoring functionality is activated.

e. Ensure that changes can only be made with the same degree of authorisation required in the initial activation of the tools.

f. Be compatible with the availability of interoperable one-stop-shop tools for guardians gathering all settings and tools.

g. Tools for guardians may include features for managing default settings, setting screen time limits (see section 6.4 on Online interface design and other tools), seeing the accounts that the minor communicates with, managing account settings, setting spending limits for the minor by default where applicable, or other features to supervise uses of the online platforms that may be detrimental to the minor's privacy, safety and security.

8 GOVERNANCE

83. Good platform governance is an effective means to ensure that the protection of minors is duly prioritised and managed across the platform, thus contributing to ensuring the required high level of privacy, safety and security of minors.

8.1 Governance (general)

84. The Commission considers that providers of online platforms accessible to minors should put in place effective governance practices as a means of ensuring a high level of privacy, safety and security for minors on their services for the purposes Article 28(1) of Regulation (EU) 2022/2065. This includes, but is not limited to:

    a. Implementing internal policies that outline how the provider of the online platform seeks to ensure a high level of privacy, safety and security for minors on its service.

    b. Assigning to a dedicated person or team the responsibility for ensuring a high level of minors' privacy, safety and security. This person or team should have sufficient resources as well as sufficient authority to have direct access to the senior management body of the provider of the online platform and should also be a central point of contact for regulators, users and trusted flaggers in matters related to minors' privacy, safety and security.

    c. Fostering a culture of privacy, safety and security for minors on the service. This includes:

        i. Fostering and prioritising a culture of child participation in the design and functioning of the platform. This should be done in safe, ethical, inclusive and meaningful ways, in children's best interests, and should provide for feedback mechanisms to explain to minors how their views have been taken into account ([74]).

(74) UNICEF's spotlight guidance on stakeholder engagement with children offers concrete steps on responsible child participation activities. UNICEF. (2025). *Spotlight guidance on best practices for stakeholder engagement with children in D-CRIAs.* Available: https://www.unicef.org/childrightsandbusiness/media/1541/file/D-CRIA-Spotlight-Guidance-Stakeholder-Engagement.pdf.

ii. Raising awareness of how the provider upholds children's rights on its platform and the risks that minors on the platform may face to their privacy, safety and/or security ([75]).

d. Providing persons responsible for minors' privacy, safety and security, developers, persons in charge of moderation and/or those receiving reports or complaints from minors, with relevant training and information ([76]).

e. Having procedures to ensure regular monitoring of compliance with Article 28(1) of Regulation (EU) 2022/2065.

f. Ensuring that any technological and organisational solutions employed to implement these guidelines are 'state-of-the-art' and are aligned with national guidance on the protection of minors ([77]), children's rights and the highest available standards ([78]).

g. Putting in place a process for the systematic collection and reporting of data on harms and risks related to privacy, safety, and protection of minors on the platform to the provider's management as well as to the person or team

(75) This approach is in line with the Better Internet for Kids strategy (BIK+), which emphasises the importance of awareness and education in promoting online safety and supports the implementation of Regulation (EU) 2022/2065 in this respect. Furthermore, the Safer Internet Centres, stablished in each Member State, demonstrate the value of awareness-raising efforts in preventing and responding to online harms and risks.

(76) This training might cover, for example, children's rights, risks and harms to minors' privacy, safety and security online, as well as effective prevention, response and mitigation practices.

(77) An Coimisiún um Chosaint Sonraí. (2021). *Fundamentals for a child-oriented approach to data processing*. Available: https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf; Coimisiún na Meán. (2024). *Online safety code*. Available: https://www.cnam.ie/app/uploads/2024/11/Coimisiun-na-Mean-Online-Safety-Code.pdf; IMY (Swedish Authority for Privacy Protection). (2021). *The rights of children and young people on digital platforms*. Available: https://www.imy.se/en/publications/the-rights-of-children-and-young-people-on-digital-platforms/; Dutch Ministry of the Interior and Kingdom Relations. (2022). *Code for children's rights*. Available: https://codevoorkinderrechten.nl/wp-content/uploads/2022/02/Code-voor-Kinderrechten-EN.pdf; CNIL. (2021). *CNIL publishes 8 recommendations to enhance protection of children online*. Available: https://www.cnil.fr/en/cnil-publishes-8-recommendations-enhance-protection-children-online; Unabhängiger Beauftragter für Fragen des sexuellen Kindesmissbrauchs. (n.d.). *Rechtsfragen Digitales*. Available: https://beauftragte-missbrauch.de/themen/recht/rechtsfragen-digitales.

(78) CEN-CENELEC (2023) *Workshop Agreement 18016 Age Appropriate Digital Services Framework*; OECD. (2021). *Children in the digital environment - Revised typology of risks*. https://www.oecd.org/en/publications/children-in-the-digital-environment_9b8f222e-en.html.

designated for the protection of minors. This is without prejudice to the obligations of providers of VLOPs stemming from Articles 34 and 35 of Regulation (EU) 2022/2065.

h. Exchanging between platforms and providers, as well as with Digital Services Coordinators, trusted flaggers, civil society organisations, academia and other relevant stakeholders, good practices and technological solutions that are aimed at ensuring a high level of privacy, safety and security for minors.

8.2 Terms and conditions

85. Terms and conditions provide a framework for governing the relationship between the provider of the online platform and its users. They set out the rules and expectations for online behaviour and play an important role in establishing a safe, secure and privacy respecting environment ([79]).

86. The Commission recalls the obligations for all providers of intermediary services as regards terms and conditions set out in Article 14 of Regulation (EU) 2022/2065, which includes the obligation for providers of intermediary services to explain the conditions for, and any restrictions on, the use of the service in a clear, plain, intelligible, user-friendly and unambiguous language. In addition, Article 14(3) specifies that intermediary services primarily directed to minors or predominantly used by them, should provide this information in a way that minors can understand ([80]) ([81]).

87. Moreover, the Commission considers that providers of online platforms accessible to minors should ensure that the terms and conditions of the service they provide:

(79) The P2089.2™ Standard for Terms and Conditions for Children's Online Engagement provides processes and practices to develop terms and conditions that help protect the rights of children in digital spheres.

(80) The Commission also recalls the requirements for video-sharing platform providers to protect minors from programmes, user-generated videos and audiovisual commercial communications which may impair their physical, mental or moral development in Article 28b of Directive 2010/13/EU. These requirements are to be evaluated and, potentially, reviewed by 19 December 2026.

(81) As indicated in the Introduction of these guidelines, certain provisions of Regulation (EU) 2022/2065 including points (5) and (6) of article 14, impose additional obligations on providers of very large online platforms ("VLOPs"). To the extent that the obligations expressed therein also relate to the privacy, safety and security of minors within the meaning of Article 28(1), the present guidelines build on these provisions.

a. Include information about:

i. The steps that users need to take from account creation to its deletion.

ii. Community guidelines that promote a positive, safe and inclusive atmosphere and that explain what conduct is expected and prohibited on their service, and what the consequences of non-compliance are.

iii. The types of content and behaviour that are considered to be harmful for minors' privacy, safety and/or security. This includes but is not limited to illegal content that is harmful for minors' privacy, safety and/or security and the dissemination of this content.

iv. How minors are protected from this content and behaviour.

v. The tools that are used to prevent, mitigate and moderate content, conduct and features that are illegal or harmful for the privacy, safety and security of minors, and the complaints process.

b. Are searchable and easy to find throughout the user's experience on the platform.

c. Do not unduly restrict any rights of minors, including their right to freedom of expression and information.

d. Are upheld and implemented in practice.

88. In addition, the Commission considers that the providers of online platforms accessible to minors should ensure changes to the terms and conditions are logged and published ([82]).

Good practice

HappyExplore is an online platform where minors can play games, create and explore creatures and worlds that they can share with each other. HappyExplore has a character called "Pixel Pioneer" which teaches users how to be responsible explorers. All users are encouraged to take the "Kindness pledge", where they learn and promise to behave kindly and safely online. Pixel Pioneer also explains the importance of moderation and safety decisions to the users as they explore the platform, such as why they should think carefully before sharing their creatures or worlds.

(82) For example, by publishing them in the Digital services terms and conditions database: https://platform-contracts.digital-strategy.ec.europa.eu/

8.3 Monitoring and evaluation

89. The Commission considers that providers of online platforms accessible to minors should adopt effective monitoring and evaluation practices to ensure a high level of privacy, safety and security for minors on their service for the purposes Article 28(1) of Regulation (EU) 2022/2065. This includes, but is not limited to:

    a. Regularly monitoring and evaluating the effectiveness of any elements of the platform that concern the privacy, safety and security of minors on the platform. This includes, for example, the platform's online interface, systems, settings, tools, functionalities and features and reporting, feedback and complaints mechanisms, and measures taken to comply with Article 28(1) of Regulation (EU) 2022/2065 ([83]). Providers should consider making these evaluations available for review and input by independent third parties such as experts or other relevant stakeholders.

    b. Regularly consulting with minors, guardians, academia, civil society organisations, child rights experts and other relevant stakeholders on the design and evaluation of any elements of the platform that concern the privacy, safety and security of minors on the platform. This should include testing these elements with minors and taking their feedback into account. To contribute to non-discrimination and accessibility, providers should, where possible, involve in these consultations minors from a diverse range of cultural and linguistic backgrounds, of different ages, with disabilities and/or additional accessibility needs.

    c. Adjusting the design and functioning of the aforementioned elements based on the results of these consultations and on technical developments, research, changes in user behaviour or policy, product and usage evolutions, and changes

(83) As indicated in the Introduction of these guidelines (section 1), certain provisions of Regulation (EU) 2022/2065 including Section 5 of Chapter III impose additional obligations on providers of very large online platforms ("VLOPs") and very large search engines ("VLOSEs"). To the extent that the obligations expressed therein also relate to the privacy, safety and security of minors within the meaning of Article 28(1), the present guidelines build on these provisions, and VLOPs should not expect that adopting the measures described in the present guidelines, either partially or in full, suffices to ensure compliance with their obligations under Section 5 of Chapter III of Regulation (EU) 2022/2065.

to the harms and risks to the privacy, safety and security of minors on their platform.

8.4 Transparency

90. The Commission recalls the transparency obligations under Articles 14, 15 and 24 of Regulation (EU) 2022/2065. In view of minors' developmental stages and evolving capacities, additional considerations concerning the transparency of an online platform's functioning are required to ensure compliance with Article 28(1) of that Regulation.

91. The Commission considers that providers of online platforms accessible to minors should make all necessary and relevant information on the functioning of their services easily accessible for minors to ensure a high level of privacy, safety and security on their services. It considers that providers of online platforms should make available to minors and, where relevant, their guardians, on an accessible interface on their online platforms the following information:

    a. Information about any measures put in place to ensure a high level of privacy, safety or security of minors on the platform. This includes information about:

        i. any age assurance methods used, how these methods work, and any third party used to provide any age verification or estimation methods.

        ii. any measures recommended in the present guidelines and put in place by the provider of the online platform.

        iii. any other measures adopted, or changes made to their services to ensure a high level of privacy, safety or security of minors on the platform.

        iv. the functioning of the recommender systems used across the platform and the different options available to users (see Section 6.5.2 on User control and empowerment).

        v. the processes for responding to any reports, feedback and complaints made or brought by minors, including indicative timeframes, and the possible outcomes and impact of these processes.

vi. the AI tools, products and features that are incorporated into the platform, their limitations and the potential consequences of their use.

vii. the registration process where one is offered.

viii. any tools for guardians that are offered, explaining how to use them and how they protect minors online [EDPB], and what types of information about the minor's online activity guardians can obtain via the use of such tools.

ix. how content that breaches the platform's terms and conditions is moderated and the consequences of this moderation.

x. how to use the different reporting, complaints, redress and support tools referred to in the present guidelines.

xi. the online platform's terms and conditions.

b. Ensure that this information, all warnings and any other communication recommended in the present guidelines are:

i. child-friendly, age-appropriate, and easily accessible to all minors, including those with disabilities and/or additional accessibility needs.

ii. presented clearly in a way that is easy to understand and is as simple and succinct as possible. For example, where the terms and conditions refer to a specific feature, the key information about this feature is presented when the minor engages with it.

iii. presented to the minor in ways that are easy to review and that provide for immediate and intuitive access, at the points at which they become relevant.

iv. presented in the official language(s) of the Member State the service is provided in.

v. engaging for minors. This may require the use of graphics, videos, and/or characters or other techniques.

vi. given to minors gradually and overtime to maximise retention by the user.

c. Any measures and changes implemented to comply with Article 28(1) of Regulation (EU) 2022/2065 could be communicated internally and made public to the extent possible

Good practice

HappyTerms is an online platform addressed at 13- to 18-year-olds. It offers minors the opportunity to participate in communities and to exchange ideas and information about shared interests. HappyTerms displays information about its terms and conditions with clear headings accompanied by explanatory icons and colourful pictures. The rules are broken down into short, easy-to-read sections and use simple language to explain the rules. There are also infographics that help minors to understand what they are agreeing to, and that pop up when they become relevant to a given feature or settings change. Users can also find rules and by clicking on "What I need to know", an icon that links the user to the relevant rules, related tools and useful links from any part of the platform. HappyTerms also offers an interactive quiz where minors can check if they have understood the terms and conditions.

9 REVIEW

92. These guidelines constitute a first interpretation by the Commission of Article 28(1) of Regulation (EU) 2022/2065. The Commission will review these guidelines as soon as this is necessary in view of practical experience gained in the application of that provision and the pace of technological, societal, and regulatory developments in this area.

93. The Commission encourages providers of online platforms accessible to minors, Digital Services Coordinators, national competent authorities, the research community and civil society organisations to contribute to this process. Following such a review, the Commission may, in consultation with the European Board for Digital Services, decide to amend these guidelines.

Annex A

5C Typology of risks

94. The OECD ([84]) and researchers ([85]) have classified the risks ([86]) that minors can encounter online, in order for providers of online platforms, academia and policy makers to better understand and analyse them. This classification of risks is known as the 5Cs typology. It helps in identifying risks and includes 5 categories of risks: content, conduct, contact, consumer risks, cross-cutting risks. These risks may manifest when there are no appropriate and proportionate measures in place to ensure a high level of privacy, safety and security, causing potential infringement of a number of children's rights.

5C typology of risks ([87])

Risks for children in the digital environment				
Risk categories	**Content**	**Conduct**	**Contact**	**Consumer**
Cross-cutting risks	Additional privacy, safety and security risks Advanced technology risks Risks on health and wellbeing Misuse risks			
Risk manifestation	Hateful content	Hateful behaviour	Hateful encounters	Marketing risks
	Harmful content	Harmful behaviour	Harmful encounters	Commercial profiling risks
	Illegal content	Illegal behaviour	Illegal encounters	Financial risks
	Disinformation	User-generated problematic behaviour	Other problematic encounters	Security risks

(84) OECD. (2021). *Children in the digital environment - Revised typology of risks*. https://www.oecd.org/en/publications/children-in-the-digital-environment_9b8f222e-en.html

(85) Livingstone, S., & Stoilova, M. (2021). *The 4Cs: Classifying Online Risk to Children*. (CO:RE Short Report Series on Key Topics). Hamburg: Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI); CO:RE - Children Online: Research and Evidence. https://doi.org/10.21241/ssoar.71817

(86) See also a risk analysis provided by the the Bundeszentrale für Kinder- und Jugendmedienschutz (BZKJ). (2022). *Gefährdungsatlas. Digitales Aufwachsen. Vom Kind aus denken. Zukunftssicher handeln. Aktualisierte und erweiterte 2. Auflage. - Bundeszentrale für Kinder- und Jugendmedienschutz*. Available: https://www.bzkj.de/resource/blob/197826/5e88ec66e545bcb196b7bf81fc6dd9e3/2-auflage-gefaehrdungsatlas-data.pdf

(87) OECD. (2021). *Children in the digital environment - Revised typology of risks*. p.7. https://www.oecd.org/en/publications/children-in-the-digital-environment_9b8f222e-en.html

95. **Content risks:** Minors can be unexpectedly and unintentionally exposed to content that potentially harms them: a. hateful content, b. harmful content c. illegal content; d. disinformation. These types of contents are widely considered to have serious negative consequences to minors' mental health and physical wellbeing, for example content promoting self-harm, suicide, eating disorders or extreme violence.

96. **Conduct risks:** Refer to behaviours minors may actively adopt online, and which can pose risks to both themselves and others such as a. hateful behaviour (e.g., minors posting/sending hateful content/messages e.g. cyberbullying); b. harmful behaviour (e.g., minors posting/sending violent or pornographic content); c. illegal behaviour (e.g., minors posting/sending child sexual abuse material or terroristic content); and d. user-generated problematic behaviour (e.g., participation in dangerous challenges; sexting).

97. **Contact risks:** Refer to situations in which minors are victims of the interactions, as opposed to the actor: a. hateful encounters, b. harmful encounters (e.g. the encounter takes place with the intention to harm the minor), c. illegal encounters (e.g. can be prosecuted under criminal law), and d. other problematic encounters. Examples of contact risks include, but are not limited to online grooming, online sexual coercion and extortion, sexual abuse via webcam, cyberbullying and sex trafficking. These risks also extend to online fraud practices such as phishing, marketplace fraud, and identity theft.

98. **Consumer risks:** Minors can also face risks as consumers in the digital economy: a. marketing risks (e.g. loot boxes, advergames.), b. commercial profiling risks (e.g. product placement or receiving advertisements intended for adults such as dating services), c. financial risks (e.g. fraud or spending large amounts of money on without the knowledge or consent of their guardians), d. security risks and e. risks related to the purchase and consumption of drugs, medicines, alcohol, and other illegal or dangerous products. Consumer risks also include risks related to contracts, for example the sale of users' data or unfair terms and conditions.

99. **Cross cutting risks**: These are risks that cut across all risk categories and are considered highly problematic as they may significantly affect minors' lives in multiple ways. They are:

a. **Advanced technology risks** involve minors encountering new dangers as technology develops, such as AI chatbots that might provide harmful information or be used for grooming by exploiting vulnerabilities or the use of biometric technologies that can lead to abuse, identity fraud, lead to exclusion etc.

b. **Health and wellbeing risks** include potential harm to minors' mental, emotional, or physical well-being. For example, increased obesity/anorexia and mental health issues linked to the use or excessive use of online platforms, which may in some cases result in in negative impacts for minors' physical and mental health and wellbeing, such as addiction, depression, anxiety disorders, deregulated sleep patterns and social isolation.

c. **Additional privacy and data protection risks** stem from access to information about minors and the danger of geolocation features that predators could exploit to locate and approach minors.

100. Other cross cutting risks ([88]) can also include:

a. **Additional safety and security risks** relate to minors' safety, particularly physical safety, as well as all cybersecurity issues.

b. **Misuse risks** relate to risks or harms to minors stemming from the misuse of the online platform, or its features.

(88) Livingstone, S., & Stoilova, M. (2021). *The 4Cs: Classifying Online Risk to Children*. (CO:RE Short Report Series on Key Topics). Hamburg: Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI); CO:RE - Children Online: Research and Evidence. https://doi.org/10.21241/ssoar.71817