EDPB Comments on the draft guidelines on protection of minors online under the Digital Services Act ('DSA')

1. Introduction

On 13 May 2025, the European Commission launched a Public Consultation[1] concerning the guidelines on protection of minors online under the Digital Services Act ('DSA'). The guidelines aim to support platforms accessible by minors in ensuring a high level of privacy, safety, and security for children, as required by DSA.

The Commission invited the European Data Protection Board ('EDPB') to provide feedback to the public consultation. The EDPB welcomes the opportunity to provide comments on the draft guidelines. The EDPB highlights that in view of the tight deadline, the present contribution constitutes solely a preliminary assessment and is without prejudice to future guidance issued by the EDPB on the application of the GDPR.

In addition, as a participant in the European Board for Digital Services' Working Group 6 on the protection of minors online, the EDPB remains available to advise the European Commission, in particular in relation to age assurance matters when data protection issues are at stake.

2. General comments

The EDPB welcomes the publication of these guidelines and notes their objective of ensuring a high level of privacy, safety and security. Children deserve special protection online: they need to be protected, respected and empowered. These principles are firmly enshrined in the GDPR, with obligations regarding the information that should be provided to children and the age required for valid consent (which may vary between 13 years old & 16 years old). It is especially important to avoid deceit or manipulation of children and to implement privacy by design & default.

The EDPB takes note that the DSA and the GDPR pursue different yet complementary objectives. While the GDPR aims to protect individuals with regard to the processing of personal data, the DSA aims to contribute to the proper functioning of the internal market for intermediary services by setting out harmonised rules for a safe, predictable and trusted online environment that facilitates innovation and in which fundamental rights enshrined in the Charter, including the principle of consumer protection, are effectively protected.

Article 2(4)(g) of the DSA states that the DSA is without prejudice to the rules laid down by other Union legal acts regulating other aspects of the provision of intermediary services in the internal market or specifying and complementing the DSA, in particular the GDPR and the ePrivacy

[1] https://digital-strategy.ec.europa.eu/en/library/commission-seeks-feedback-guidelines-protection-minors-online-under-digital-services-act

Directive. Recital 10 of the DSA specifies that the protection of individuals with regard to the processing of personal data is governed by the rules of Union law on that subject, in particular the GDPR and the ePrivacy Directive.

The safety and security of children online is a major and growing concern that must be balanced with the need to respect the privacy and the protection of personal data of all internet users, including children. While many of the risks and measures mentioned by the Commission are relevant for both minors and adults, risks stemming from the design or functioning of online platform services are generally higher for children than for adults.

It is also crucial that children do not access harmful content. Age assurance is one of the tools to avoid this. There are three primary categories of age assurance: age estimation, age verification and self-declaration[2]. In this regard, the EDPB has previously expressed serious doubts as to the effectiveness of self-declaration as a method of age assurance within the context of high-risk processing[3]. Furthermore, the EDPB notes that while age estimation is less precise than age verification, it may also entail a higher degree of interference with users' fundamental rights to data protection, as it may entail large scale processing to profile users with a view to determine the likelihood that they are minors.

In recognition of the importance of a consistent approach at the EU level on the topic of age assurance, the EDPB issued specific guidance under the GDPR in the form of 10 principles that should be taken into consideration when personal data is processed in this context. These principles aim to support the different parties involved in age assurance to ensure its implementation respects the fundamental rights and freedoms of natural persons'.

Furthermore, the EDPB considers that the proportionality assessment of evaluating the impact of measures on children and, all individuals'rights and freedoms enshrined in the Charter of fundamental rights of the European Union, should also include specific reference to the respect of the fundamental rights to privacy and data protection.

The EDPB statement is focused on online use cases, including when a minimum age is prescribed by law or results from terms and conditions of service of the platform, for buying products, for using services that may harm children or for performing legal acts; and when there is a duty of care to protect children (for example, to ensure that services are designed or offered in an age-appropriate way). DPAs also have the important task to promote awareness and understanding of risks among children.

Overall, the Commission's draft guidelines provide very clear and practical recommendations on what measures providers of online platforms should take to improve the security, safety and privacy of minors according to Article 28(1) DSA. The EDPB welcomes the clarification of the material scope of Article 28 (platforms accessible to minors).

The EDPB intends to provide additional guidance on data protection compliance on this subject matter in the context of its 'Children's guidelines[4] and of its Guidelines on the interplay between GDPR and DSA. [5]

As a preliminary remark, the EDPB recommends highlighting in the introduction of the draft Commission guidelines that all measures adopted by providers of online platforms to comply with

[2] EDPB Statement 1/2025 on age assurance, Adopted on 11 February 2025.
[3] EDPB Binding Decision 2/2023 on the dispute submitted by the Irish SA regarding TikTok Technology Limited (Art. 65 GDPR), Adopted on 2 August 2023, paragraph 228.
4 EDPB Strategy 2024-2027
[5] Ibid.

Article 28(1) DSA should also comply with the GDPR and that that DPAs are solely competent to assess such compliance. Therefore, a reference to the importance of cooperation between all competent regulators and authorities might be beneficial, to ensure that Article 28(1) DSA and GDPR requirements are applied in a consistent and coherent manner.

The EDPB comments focus primarily on Section 6 of the draft guidelines ('Service Design'). For the sake of clarity, this contribution comprises (i) the present cover letter providing general comments the EDPB wishes to make and (ii) an annex where comments of a more technical nature are made directly to the draft guidelines in order to provide some examples of possible amendments. The EDPB comments range from general remarks to more concrete suggestions on parts of the guidelines.

EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR COMMUNICATIONS NETWORKS, CONTENT AND TECHNOLOGY

Platforms Policy and Enforcement
Digital Services

Communication from the Commission

Commission 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

FOR PUBLIC CONSULTATION 13 MAY - 10 JUNE 2025

1 INTRODUCTION

Online platforms are increasingly accessed by minors ([6]) 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.

There is, however, wide consensus among policy makers, regulatory authorities, civil society, researchers, educators and guardians ([7]) that the current level of privacy, safety and security online of minors is often inadequate. The design and features 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 ([8]) 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 related to extensive use or overuse of online platforms and exposure to inappropriate or exploitative practices, including in relation to gambling. 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 affect a minor's privacy, safety and security ([9]). 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.

These guidelines aim to support providers of online platforms in addressing these risks by providing a set of measures that the Commission considers will help providers to ensure a high level of privacy, safety and security on their platforms. 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 ([510]) 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.

[66] In the present guidelines, 'child', 'children' and 'minor' refer to a person under the age of 18.

[7] In the present guidelines, 'guardians', refer to persons holding parental responsibilities.

[8] Illegal content includes but is not limited to content depicting illicit drug trafficking, terrorist and violent extremist content and child sexual abuse material.

[9] 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.

[10] See section 6.1 on age assurance.

Adopting these and other measures – on matters 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

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 ([11]).

Paragraph 1 of that 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 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.

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 ([12]). 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*".

As regards the first scenario described in that recital, the Commission considers that a provider of an online platform that simply declares in its terms and conditions that it is not accessible to minors but does not put any effective measure in place to avoid that minors access its service, cannot claim that its online platform falls outside the scope of Article 28(1) of Regulation (EU) 2022/2065 for that simple reason. 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 year, will nevertheless be considered

[11] 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.

[12] 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.

accessible to minors within the meaning of Article 28(1) of Regulation (EU) 2022/2065 where users under the age of 18 in fact access their service.

As regards the third scenario, recital 71 of Regulation (EU) 2022/2065 explains that one example of a situation in which a provider of 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, and this reveals that some of those recipients are minors. Other examples of situations in which a provider may be aware that some of the recipients of its online platform service are minors 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 and where the provider of the online platform has conducted or commissioned research that identifies minors as recipients of its service.

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 ([13]).

Other provisions of Regulation (EU) 2022/2065 are also aimed at ensuring the protection of minors online ([14]). 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") ([15]). 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 and VLOSEs 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)

Commented [A1]: Suggestion to add an example of this here i.e. an age stated in a social media bio.

Commented [A2]: The guidelines and the DSA are not very clear about whether online platforms have to pro-actively determine how many children are actually accessing the service of an online platform. The word 'may' in 77 seems to imply that there isn't such an obligation, while on the other hand the guidelines seem to imply that the amount of minors should be taken into account in the proportionality assessment ('user base of the service' chapter 4) and the risk assessment ('number and type of users' chapter 5). We therefore ask the Commission to be more clear on this part and to also mention that any processing of personal data that is needed for the purpose of 28(1) should be in line with the GDPR. The EDPB intends to issue guidance providing elements on whether a website is accessed by minors in the context of the Guidelines on Children's processing of personal data.

[13] 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,

[14] 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.

[15] 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.

2022/2065, as those providers may need to put in place 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 ([16]).

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 ([17]). 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 those instruments.

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 everyone contributes to privacy, safety and security online of minors.

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.

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 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. Nevertheless, adopting and implementing measures set out in these guidelines, either partially or in full, shall not automatically entail compliance with that provision.

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.

Commented [A3]: We would like to see more firmly, in line with the text of the DSA, that these are guidelines are without prejudice to, amongst others, the GDPR and ePrivacy regulation.

Commented [A4]: There are several references to ensuring high levels of privacy throughout these guidelines, which makes sense of course given the text of Article 28. However, there will be instances where certain of the measures proposed by the Commission may fall to the competence of Data Protection Authorities under the GDPR. With that in mind, it would be beneficial if we could add some sort of reference here to that fact that adherence to these guidelines doesn't necessarily mean that a company's measures are fully in compliance with data protection law. DPAs are solely competent to assess compliance with the GDPR.
The EDPB also recommends making a reference to the importance of cooperation between competent authorities under the DSA and DPAs, to ensure that Article 28(1) DSA and GDPR requirements are applied in a consistent and coherent manner.
In particular, in light of CJEU case law (C-252/21), when authorities with competences for the enforcement of the DSA (including the European Commission) are called upon, in the exercise of their powers, to examine whether the conduct of a provider of an online platform (e.g., in the context of implementation of Article 28(1) DSA) is consistent with the provisions of the GDPR, they should consult and cooperate sincerely with the national DPA concerned or with the lead DPA.

[16] 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.

[17] 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 wellbeing, 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 recall as well the European Commission Fitness Check of EU consumer law on digital fairness.

3 STRUCTURE OF THE GUIDELINES

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

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 ([18]) or technical standards ([19]). 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

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:

- **Proportionality**: 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 for all providers of online platforms to apply all the measures described in these guidelines.

In order to be proportionate, measures put in place by providers of online platforms should be targeted to those specific elements of online platforms - whether content, areas or features - that pose identifiable risks to users. . Determining whether a particular measure is proportionate in particular where it entails an interference with individuals' fundamental right to data protection will require a case-by-case review by each provider (i) of the risks to

Commented [A5]: We suggest that the Commission give more guidance on what aspects should be *concretely* taken into account when doing this assessment. For example: what is meant with 'user base of the service'? Does that mean that the proportion of minors of the user base should be taken into account? And what does the 'type of service' mean and how is this important for the proportionality assessment?

[18] 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 children's personal data in accordance with Regulation (EU) 2016/679 (GDPR).

[19] 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

minors' privacy, safety and security stemming from its online platform or parts of it, considering *inter alia* the type of service it provides and its nature, its intended or current use, and the user base of the service, and (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") including on all users' fundamental rights to privacy and data protection (see Section 5 on Risk review).

- **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 ([20]). 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, it is necessary to consider all children's rights, including their right to protection, non-discrimination, inclusion, participation, privacy, information and freedom of expression, among others.
- **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 design, development and operation of their services ([21]).
- **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 ([22]).

5 RISK REVIEW

Where a provider of an online platform accessible to minors is determining which measures are appropriate and proportionate to ensure a high level of safety, privacy and

Commented [A6]: See comment above, i.e. proposal to add a sentence, since the proportionality test should be assessed against the specific risk.

Commented [A7]: The EDPB welcomes the risk-based approach to assessing the need for an age assurance mechanism and choosing the most appropriate one to protect children on online platforms. We consider that more clarity is needed on the link between the conclusion of the risk assessment and the measures described in Section 6.

[20] 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-andrecommendations/general-comment-no-25-2021-childrens-rights-relation

[21] 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/guidelines42019-article-25-data-protection-design-and_en

[22] This requires prioritising features, functionality, content or models that are compatible with children's evolving capacities. 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. *Cfr* CEN-CENELEC (2023) *Workshop Agreement 18016 Age Appropriate Digital Services Framework*, and ages and developmental stages available, *inter alia* as Annex to the Dutch Children's Code: https://codevoorkinderrechten.nl/wpcontent/uploads/2022/02/Code-voor-Kinderrechten-EN.pdf

security to minors on their platform, the Commission considers that that provider should, at a minimum, identify:

- How likely it is that minors will access its service.
- The risks to 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. 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.
- The measures that the provider is already taking to prevent and mitigate these risks.
- 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.
- 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 disproportionately or unduly restricted. Children's and 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.

When conducting this review, providers of online platforms accessible to minors should be ~~guided~~ informed by the best interest of the minor ([23]).

Providers should carry out the review whenever they make significant changes to their online platform and should consider publishing its outcomes.

Existing tools to carry out child rights impact assessments can support providers in carrying out this review ([24]). 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.

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

Commented [A8]: Important to flag that providers will also have obligations pursuant to the GDPR in terms of assessing risk of a service and that compliance with these guidelines does not obviate a controller from their data protection compliance obligations, e.g. having to carry out a DPIA.

Commented [A9]: It is important to note that, in the context of the proportionality assessment, the best interest of minor users may be in tension with fundamental rights of other users.

Commented [A10]: Suggestion to make a reference to 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

Commented [A11]: Impact on children's rights is only a part of the proportionality assessment, as providers of online platforms should also assess the impact of the measures they deem to put in place for the protection of minors' safety, security and privacy on the rights of other users.

[23] 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.

[24] Dutch Ministry of the Interior and Kingdom Relations (BZK). (2024). *Child Rights Impact Assessment (Fillable Form).* Available: https://www.nldigitalgovernment.nl/document/childrens-rights-impactassessment-fill-in-document/; 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/reports/CRIA-responsibletech

6 SERVICE DESIGN

6.1 Age assurance

6.1.1 Introduction and terminology

The Commission considers measures restricting access based on the recipient's age to be an effective means to ensure a high level of privacy, safety and security for minors on online platforms, where those measures are used to protect minors from accessing age inappropriate content online, such as gambling services or pornography, or from being exposed to risks such as grooming.

Such measures are commonly referred to as "age assurance" ([25]). 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.

- **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.
- **Age estimation** consists of independent 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 ([26]).
- **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.

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 in principle down to the day, age estimation provides an approximation of the user's age.

6.1.2 Determining whether to put in place age assurance measures

Before deciding whether to put in place any age assurance method, providers of online platforms accessible to minors should always conduct an assessment to determine whether such a method 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 ([27]). In this regard, the Commission is of the view that providers should also consider other measures set out in other sections of these guidelines as an alternative to age assurance measures.

[25] 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

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

[27] The review of risks and balancing of rights exercise outlined in Section 5 on Risk review can help providers of online platforms to conduct this assessment.

Commented [A12]: On this point, the EDPB, in its Statement on age Assurance, recommends that due account be taken of technologies and architectures that favour data held by users and the local and secure processing of this data (on the user's terminal). It also recommends the use of solutions such as cryptographic protocols (proof of zero disclosure of knowledge) or batches of single-use identifiers (footnote: Statement 1/2025 on Age Assurance, §34).

Commented [A13]: Another important difference is that, although age estimation is less precise than age verification, it may entail a higher degree of interference with users' fundamental rights to data protection, as it may entail large scale processing to profile users, with a view to determine the likelihood that they are minors.
Therefore, we propose to generally discourage the use of algorithmic age estimation because of the current high rates of false positives and negatives, and the significant degree of interference with users' fundamental right to data protection.

Commented [A14]: See comment above on part 5.

Such an assessment is important because it ensures that any restriction to the exercise of fundamental rights and freedoms is proportionate.

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 an age assurance method as proximate to these as possible.

5

6.1.3 Determining which age assurance methods to use

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:

- 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:
  - the sale of alcohol,
  - access to pornographic content,
  - or access to gambling content.
- Where 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, due to identified risks to minors, even if there is no formal age requirement established by law.
- 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 contact risks as well as content risks, that cannot be mitigated by other less intrusive measures[28]).

Methods that rely on verified and trusted government-issued IDs 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, ([29]) which will provide a safe, reliable and private means of digital identification within the Union.

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.

To facilitate age verification before the EU Digital Identity Wallet becomes available, the Commission is currently working on an EU age verification solution as a standalone age

[28] These risks can be identified via the review of risks set out in Section 5.

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

Commented [A15]: In the section on the choice of the most appropriate mechanism, it should be indicated that the implementation of an age assurance mechanism may involve processing operations covered by the legal framework of Article 22 of the GDPR (decisions based solely on automated processing and appropriate measures to safeguard the data subject's rights and legitimate interests). In this respect, reference should be made to Section 2.7 of the EDPB's Statement on age assurance.

Commented: [A16]: Suggestion to provide an example.

Commented [A17]: The way we understood it, the Wallet will not neccesarily have the capacities to facilitate age verification. If this is indeed the case we see no reason to include a hint at the wallet in this chapter. Identifying the user instead of only checking their age is a privacy risk in and of itself.

If the Wallet will definitely feature age verification, we suggest adding a description of the specific functionality in this space and possibly precise that the Wallet has the capacities to implement selective disclosure of attributes (that aligns with minimisation principle, ZKP, …).

verification measure. Once finalized, the EU age verification solution will aim to provide a valid example and a benchmark for a device-based method of age verification.

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.

Users can 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.

While 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, those methods should ensure an equivalent level of verification and data protection as the EU age verification application.

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:

- Where the 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~~ due to the provider's assessment of when the online platform is safe and secure for minors to use ([30]) ([31]).

[30] 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.

[31] In some cases, it may be possible for the provider to verify that the minor was signed up by their guardians.

Commented [A18]: According to our understanding, the EU age verification solution isn't intended to address the +/- 13 use case. It's only designed to determine whether someone is under or over 18. Therefore this solution, at least in its first iteration, won't be usable for the 3rd example given above of where AV is considered appropriate:

Any other circumstances in which the provider of an online platform accessible to 260 minors has identified high risks to minors' privacy, safety or security, including 261 contact risks as well as content risks, that cannot be mitigated by other less intrusive

It's also unclear whether the final Digital Wallet will address the +/- 13 use case, so what does the Commission propose to be a suitable age verification method in this instance?

Commented [A19]: Can the Commission give examples of appropriate age estimation methods?

Commented [A20]: We suggest to change the wording according to the bullets regarding age verification. There are several reasons why service providers may set minimum ages in their terms and conditions, other than there being risks for children under a certain age on the platform (e.g. national laws or the legal capacity of minors). An age limit therefore not necessarily indicates the platforms safety and security for minors. We strongly suggest the change made, since it would include all scenarios where risks to minors are not the reason why a minimum age is set - rendering age assurance not proportionate in that case. As to the assessment, will it be shared with the Commission and the DSC?

- 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) ([32]) 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 age verification but not low enough that it would be appropriate to have no age assurance methods in place at all.

Providers of online platforms accessible to minors that are confronted with those two scenarios may also opt to put in place age verification methods ~~instead~~additionally. In any event,

providers should conduct a proportionality assessment justifying the adoption of age assurance measures prior to putting them in place.

Since data processing has to be lawful, it is notable that Art. 28(3) of Regulation (EU) 2022/2065 states that providers of online platforms are not obliged to process additional personal data in order to assess whether the user is a minor in order to comply with Article 28(1). Therefore, ~~W~~

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 ([33]).

The implementation of different, alternative age assurance measures also ensures accessibility for users that may not be able to use a certain verification or estimation method due to e.g. not having access to the documents needed for a verification.

Recommended measure	**Scenarios**
Age verification only	• 18+ restricted content and goods, such as pornography and gambling platforms • Services designed for an adult audience only, such as adults dating platforms, posing risks to minors • 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)

Commented [A21]: The EDPB notes that although age estimation is less precise than age verification, it may entail a higher degree of interference with users' fundamental rights to data protection, as it may entail large scale processing to profile users, with a view to determine the likelihood that they are minors. How is a "high risk" defined?

Commented [A22]: We welcome the reference to the EDPB statement and we consider that since in all instances there will be processing of personal data this paragraph could be even stronger. In this regard, to provide readers with more information on why this statement is important, we suggest adding: *"Since data processing has to be be lawful, it is notable that Art. 28(3) of Regulation (EU) 2022/2065 states that providers of online platforms are not obliged to process additional personal data in order to assess whether the user is a minor in order to comply with Article 28(1).''*

[32] These risks can be identified via the review of risks set out in Section 5.

[33] See EDPB statement 1/2025 on Age Assurance. Available: https://www.edpb.europa.eu/system/files/2025-04/edpb_statement_20250211ageassurance_v12_en.pdf

Age estimation or age verification	• Terms and conditions requiring minimum age lower than 18 to access the service, ~~which indicates that the provider has assessed their platform to be safe and secure~~ due to identified risks ~~to use~~ for minors ~~above~~ under the indicated age • Medium risk services - age assurance is used to ensure age -appropriate experiences for minors online

Good practice

MegaBetting ([34]) 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 an 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 application on the user's phone and. The provider considers therefore that the system meets the criteria of being highly effective whilst preserving the privacy of the user.

299

300

Commented [A23]: This wording is framing the requirement differently than the one above and also introduces a new argument of the service being safe for children over the minimum age. We suggest changing the wording according to the one above.

[34] All good and poor practice examples in these guidelines refer to fictious online platforms.

Poor practice

SadMedia is a social media online platform. The provider of SadMedia decided to restrict its services to minors who are at least 16 years old. This was based on its assessment of the 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 requirement 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.

Commented [A24]: We think this example could be improved by referencing the degree of risks that are posed by SadMedia's service. Otherwise, it's unclear as to what is an acceptable margin of error for age estimation in the context of social media.

Where a platform has determined that age assurance is necessary to achieve a high level of privacy, safety and security for minors on their service, it should always make more than one age assurance method available. 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, at least two different age verification or estimation methods, or one verification and one estimation method, should be provided ([35]). Furthermore, providers of online platforms should provide a redress mechanism for users to complain about any incorrect age assessments by the provider ([36]).

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 effectiveness of any age assurance method

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

[35] See also point 17 of the EDPB Statement on age assurance.

[36] 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.

- **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 metrics to evaluate the extent to which it can correctly determine the age or age range of a person ([37]). Providers of online platforms should periodically review whether the technical accuracy of the method used still matches the state-of-the-art.

- **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 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.

- **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.

- **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 ([38]). According to the European Data Protection Board, and in line with Article 28(3) of regulation 2022/2065 ([39]), 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~~should not~~ provide additional means for providers to identify, locate, profile or track natural persons ([40]). 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 the

Commented [A25]: This is misquoted: 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… etc.

[37] 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.

[38] 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.

[39] 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.

[40] See EDPB statement 1/2026 on Age Assurance point 2.3 and 2.4.

extent to which the method provides transparency about the process and/or puts information about the user at risk.

- **Non-discrimination.** How a given method can discriminate against some users. 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 and minority backgrounds.

The Commission considers that **self-declaration** ([41]) 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.

Furthermore, where a third party is used to carry out age verification or estimation, the Commission considers that this should be explained as in every case to minors 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

Registration or authentication may influence whether and how minors are able to access a given service in a safe, age-appropriate and rights-preserving way. 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:

- Explain to users the benefits of registration or why registration is necessary.
- Ensure that the registration process is easy for all minors to access and navigate, including those with disabilities or additional accessibility needs.
- Ensure that the registration process includes measures to help users understand whether they are allowed to use the service and measures to reduce the risk of them making further attempts to register if they are below the minimum age required by the online platform accessible to minors ([42]).
- Avoid encouraging or enticing users who are below the minimum age required by the online platform accessible to minors to create accounts.
- Ensure that it is easy for minors to log out and to have their profile deleted at their request.

Commented [A26]: Any method being used should provide the requisite information under Article 12 GDPR, it's not a matter of "the extent to which"? Could the Commission clarify?

Commented [A27]: Transparency information should be provided to children regardless of whether a third party is being used or not.

Commented [A28]: There are also data protection obligations to consider here. Would the Commission consider adding a footnote that more obligations arise in relation to controller/processor relationships?

[41] 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; Coimisiún na Meán. (2024). *Online safety code*. Available: https://www.cnam.ie/app/uploads/2024/11/Coimisiun-na-Mean-Online-Safety-Code.pdf

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

- Use the registration process as one of the main opportunities to highlight the safety features of the platform or service, any identified risks to a minor's privacy, safety or security and resources available to support users.

6.3 Account settings

6.3.1 Default settings

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 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 ([43]).

The Commission therefore considers that providers of online platforms accessible to minors that use default settings 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 should:

- Ensure that privacy, safety and security by design principles are consistently applied to all account settings for minors.
- 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 that:
  - accounts of minors only allow interaction such as likes, tags, comments, direct messages, reposts and mentions by accounts they have previously accepted as "friends" or contacts. This categorisation requires regular review.
  - No account, except the minor's, can download or take screenshots of content uploaded or shared by the minor to the platform.
  - only accounts that the minor has previously accepted as contacts can see their content and posts.
  - geolocation, microphone and camera, contact synchronisation as well as all ~~optional~~ non-strictly necessary ~~-~~tracking features are turned off.
  - profiling for ~~,~~ behavioural targeting ~~and personalization of content~~ ~~are~~is turned off.

[43] 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.

- the default autoplay of videos and hosting live streams are turned off.
- 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).
- features that may contribute to excessive use, such as the number of "likes" or "reactions", communication "streaks", the "... is typing" function, ephemeral content, and "read receipts," are turned off.
- any functionalities that increase users' agency over their interactions are enabled by default. 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.
- filters that can have detrimental effects on body image, self-esteem and mental health are turned off.

- Regularly test and update default settings, ensuring that they remain effective 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).
- Ensure that users' choices about settings remain effective after updates or changes to their service.
- Ensure that minors are not in any way encouraged or enticed to change their settings to lower levels of privacy, safety and security.
- Ensure that minors are provided with incremental degrees of control over their settings, according to their age and needs. ([44])
- 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).

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

Commented [A29]: With a view to offering settings that encourage minors to take greater control of their own data, the EDPB suggests that the recommendation mentioned here be clarified by referring to the EDPB guidelines on transparency and giving examples of good practice (for example, setting up a help centre for minors with information leaflets).

[44] 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/Codevoor-Kinderrechten-EN.pdf

- 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
- Actively and continuously raise awareness and seek agreement from minors and ask for their choices to be reaffirmed or modified at certain points.
- Present age-appropriate warning signals clearly explaining the potential consequences of any changes.
- Automatically turn off geolocation, microphone and camera as well as ~~optional~~ tracking features after the session ends, if a minor turns them on.

Commented [A30]: As above.

6.3.2 Availability of settings, features and functionalities

Providers of online platforms accessible to minors may remove settings, features and functionalities altogether to ensure a high level of privacy, safety and security of minors for the purposes Article 28(1) of Regulation (EU) 2022/2065. In those circumstances, the Commission considers that those providers should put measures in place which:

- Ensure that minors cannot easily be found or contacted by accounts they have not previously accepted as contacts. This includes ensuring that minors' personal contact data, location data, telephone number and other content facilitating direct communication are not disclosed to accounts that the minor has not accepted as contacts.
- Ensure that minors' accounts are not included in contact suggestions to other users. Adult accounts or accounts likely to be fake minor accounts should not be recommended to minors.
- Ensure that only accounts that the minor has previously accepted as contacts can see their profile information, biography, lists of friends and followers and accounts that the minor follows, and that such information as well as previous history becomes unavailable if the account is blocked or otherwise un-accepted.
- Ensure that minors are provided with the possibility to restrict the visibility of individual pieces of content that they publish, as well as the possibility to restrict the visibility of their content generally.

Commented [A31]: Again, important to highlight that measures like this also fall within the scope of data protection framework.

When assessing whether any additional settings, features or functionalities should be removed from minors' accounts altogether to ensure a high level of privacy, safety and security of minors, the Commission considers that 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.

6.4 Online interface design and other tools

Commented [A32]: In the section on interfaces (section 6.4), reference could be made to the EDPB guidelines on dark patterns, which have sections dedicated to children (in particular paragraph 7). In general, deceptive designs of the 'emotional steering' type, which encourage the user to share more data, should be avoided for children. In this respect, the guidelines on dark patterns give specific examples.

The Commission considers that putting in place measures allowing minors to take control of their online experiences is an effective means of ensuring a high level of privacy, safety and security of minors for the purposes Article 28(1) of Regulation (EU) 2022/2065.

Commented [A33]: This potentially reads as though it's an effective ***singular*** way that doesn't require additional measures, would suggest rewording for clarity. "is an effective means of contributing towards a high level…"

Without prejudice to the obligations of providers of VLOPs and VLOSEs 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. This could include, for example:

- Ensuring that minors are not exposed to persuasive design features that are aimed predominantly at engagement or that may lead to extensive use or overuse of the platform or the forming of 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 ([45]), and the creation of virtual rewards for performing ~~repeated~~ actions on the platform.

- Introducing customisable, easy-to-use, child-friendly and effective time management tools (see Section 6.4 on Online interface design and other tools) to increase minors' awareness of their time spent on online platforms and help them engage with the service for no longer than they or their guardians intend. In order 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.

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

Commented [A34]: We wonder if there is a specific reason why only repeated action would be barred from being rewarded with virtual items. In our view, this should apply to any action that a child takes on an online platform.

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

[45] 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.

trust. Minors are groomed and coerced into creating and sharing child sexual abuse images with their abusers.

6.5 Recommender systems and search features

Recommender systems determine the manner in which information is prioritised and presented 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 minors' privacy, safety and security online by, for example, amplifying content that can have a negative impact on minors' safety and security ([46]).

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 ([47]).

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

Providers of online platforms accessible to minors that use recommender systems, including search features, in the provision of their service should:

- Take into account specific needs, characteristics, disabilities and additional accessibility needs of minors when defining the objectives, parameters and

[46] Munn, L. (2020). Angry by design: Toxic communication and technical architectures. *Humanities and Social Sciences Communications, 7*(53). Available: https://doi.org/10.1057/s41599-02000550-7; 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

[47] 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.

evaluation strategies of recommender systems, in particular by not only optimising or predominantly maximising time spent on, engagement and interaction with the platform. Parameters and metrics related to accuracy, diversity, inclusivity and fairness should also be considered.

- Ensure that recommender systems promote minors' access to information that is relevant and adequate for them, with due consideration to their age group.
- Ensure that recommender systems do not rely on ~~the~~ on-going 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, and do not rely on the collection of any behavioural data that captures the user's activities off the platform.
- Prioritise 'explicit user-provided signals' over 'implicit engagement-based 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, 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 ([48]), and other quality based signals. For the purposes of the present guidelines, 'implicit engagement-based signals' shall be understood as referring to ambiguous signals that infer user preferences from their activities (browsing behaviour on a platform), such as time spent viewing content and click-through rates.
- Implement measures to prevent a minor's repeated exposure to content that could pose a risk to minors' 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, illegal content and distressing content depicting violence or encouraging minors to engage in dangerous activities.
- Put in place measures to reduce the risk that content is recommended which poses risks to minors' privacy, safety or security, or that has been reported or flagged by users, trusted flaggers or other actors or content moderation tools, and whose lawfulness and adherence to the platforms' terms and conditions have not yet been verified (see Section 6.7 on Moderation for more information).
- Implement measures to ensure that recommender systems do not enable or facilitate the dissemination of illegal content or the commitment of criminal offences against minors.
- 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.

Commented [A35]: Suggestion to clarify what the reference to on going collection means in practice. Again, worth mentioning that this is something that also falls within the scope of the data protection frameworks.

Commented [A36]: This falls also within remit of the data protection framework.

Commented [A37]: Due consideration should be given to data minimization and transparency here.

Commented [A38]: Namely profiling. A connection to GDPR would be good here: The EDPB has also recognised that in certain circumstances, targeted advertising based on profiling may fall within the prohibition in Article 22 because it may have significant effects e.g. on vulnerable adults or minority groups. In a similar vein, the EDPB has also recognised that children can be particularly susceptible in the online environment and more easily influenced by behavioural advertising.

[48] 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.

- 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 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 ([49]).

6.5.2 User control and empowerment

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

- Provide minors with the opportunity to reset their recommended feeds completely and permanently.
- Provide prompts for the minor to search for new content after a certain amount of interaction with the recommender system.
- Ensure that minors can choose an option of their recommender system that is not based on profiling.
- Ensure that relevant reporting and feedback mechanisms set out in Section 7.1 of the present guidelines 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 reducing the visibility of similar content and accounts.

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:

- 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. Providers should also provide information to minors about prompts that encourage minors to search for new content after a certain period of time interacting with the recommender system. This information should be child-friendly and accessible (see Section 8.4 on Transparency).
- Ensure that any settings and information provided to minors about their recommender systems are presented in child-friendly and accessible ways (see Sections 6.4 on Online interface design and other tools and Section 8.4 on Transparency for more details).
- 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 throughout the user's time on the platform. These preferences should directly influence the recommendations

Commented [A39]: It is unclear to us what is meant with the option to reset your feed permanently. Does that mean that children should always have an option to reset their feed or that they should be allowed to reset their feed once and for all? Might be useful to clarify this.

[49] 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 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.

provided by the system, ensuring that they align more closely with the minor's age and best interests ([50]).

6.6 Commercial practices

Minors are particularly exposed to the persuasive effects of commercial practices and have a right to be protected against economically exploitative practices ([51]). Despite this, minors are confronted with commercial practices everywhere online, facing diverse, dynamic and personalised persuasive tactics through, for example, advertisement, product placements, the use of in-app currencies, influencer marketing or AI-enhanced nudging ([52]). This can have a negative effect on minors' privacy, safety and security when using the services of an online platform.

In line with, and without prejudice to, the existing horizontal legal framework([53]) and the more specific rules in Regulation (EU) 2022/2065 on advertising (Articles 26 and 28(2)) or 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:

- 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.

[50] See Articles 27(1) and (3) of Regulation (EU) 2022/2065.

[51] 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

[52] 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

[53] 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.

- Have a responsible marketing and advertising policy in place that does not allow harmful, unethical and unlawful advertising ([54]) 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.
- Ensure that declarations of commercial communication are clearly visible, child-friendly 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.
- 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 (see Section 5 on Risk review).
- 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 ([55]). In this context, the Commission recalls that providers of online platforms 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 ([56]). Examples of disguised commercial communications 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.
- Ensure transparency of economic transactions in an age-appropriate way and avoid the use of intermediate virtual currencies, such as tokens or coins, that can be exchanged with real money and then used to buy other virtual items, which can have the effect of reducing transparency of economic transactions and may be misleading for minors.
- Ensure that minors, when accessing online platforms or parts and features thereof that are presented or appear as being free ([57]), are not exposed to in-app or in-game purchases that are or appear to be necessary to access or use the service.

[54] 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.

[55] 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.

[56] 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.

[57] 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.

- Ensure that minors are not exposed to practices that can lead to excessive or unwanted spending or addictive behaviours, by ensuring that virtual items such as loot boxes, other products with random or unpredictable outcomes or gambling like features are not accessible to minors, and by introducing separation or friction between content and the purchasing of related products.
- Ensure that minors are not exposed to manipulative design techniques ([58]), such as scarcity ([59]), intermittent or random rewards, or persuasive design techniques, ([60]).
- Ensure that minors are not exposed to unwanted purchases, e.g. by considering deploying effective tools for guardians (see Section 7.3 on Tools for guardians).

6.7 Moderation

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.

The Commission recalls the obligations related to terms and conditions set out in Article 14 of Regulation (EU) 2022/2065 and to transparency reporting provided in Article 15 of that Regulation for providers of intermediary services, which includes providers of online platforms; and the obligations related to trusted flaggers ([61]) 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 +, which constitutes a code of conduct within the meaning of Article 45 of Regulation (EU) 2022/2065. 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:

- Define clearly and transparently what the platform considers as content and behaviour that is harmful for minors' privacy, safety and security, ideally in cooperation with independent experts and civil society. This should include any content and behaviour that is illegal under EU or national law. Providers of online platforms accessible to minors should always ensure that their terms and conditions

[58] As set out in Article 25 of Regulation (EU) 2022/2065.

[59] 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.

[60] 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.

[61] 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.

clearly define harmful content and behaviour and do not unduly restrict any rights of minors, including minors' right to freedom of expression and information.

- 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 and ensure that these policies and/or procedures are enforced in practice.
- Take into account the following factors when prioritising moderation: the likelihood of the content causing harm to a minor's privacy, safety and/or security, the impact of the harm on that minor, and the number of minors who may be harmed.
- Consider human review for content that substantially exceeds the average number of views and for any reported accounts that the provider suspects may pose a risk of harm to minors' privacy, safety or security.
- Put in place effective technologies, internal mechanisms and preventative features to reduce the risk of content and behaviour that are harmful to minors' privacy, safety of security from being shown to minors in their accounts' interface or other functionalities of the service, including:
    - 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.
    - Integrating into any generative 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.
    - 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.

Commented [A40]: It might be useful to add more guidance on this topic.

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

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.

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.

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:

- Implement reporting, feedback and complaints mechanisms that:
  - are effective, child-friendly and accessible (see Section 6.4 on Online interface design and other tools)
  - 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).
  - 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.
  - Allow all users to report a suspected underage account, where a minimum age is stated in the platform's terms and conditions.
  - 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 ([62]).

Commented [A41]: Article 28 (1) DSA is intended to provide protection to minors, and not for all kinds of commercial purposes. The measures in question should therefore be considered in that specific framework. Given the circumstance that the feedback from minors in the context of recommender systems is intended to protect minors against certain unwanted and / or inappropriate content, the EDPB is of the opinion that such information may not be used for the (commercial) purpose of (fine-tuning) personalized (targeted) advertisements to minors, or to enrich the user profile for commercial purposes.

[62] See section 6.5 of the present guidelines for information about how this information should affect the provider's recommender systems.

- 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.

- Ensure that the reporting, feedback and complaints mechanisms established under Article 20 of Regulation (EU) 2022/2065 ([63]):
  - Contribute to a high level of privacy, safety and security for minors.
  - Are aligned with fundamental rights, in particular children's rights.
  - Are available for intuitive and immediate access for all minors, including for those with disabilities and/or additional accessibility needs.
  - Are easy for minors to use and understand, are age-appropriate and engaging (see Section 6.4 on Online interface design and other tools). Providers could, for example, state that reporting is confidential and useful for users.
  - Are available for non-registered users if they may access the online platform's content.
- If reporting categories are used, ensure that they are adapted to the youngest users allowed on the platform. Complex menu systems should be avoided. There should also be an option available that allows minors to provide their own reasons for a report.
- Provide minors with easy access to information about whether the provider of the online platform discloses reports and/or complaints to other users.Where providers of online platforms share information with others, they should explain to minors when, how and what information related to reports and/or complaints they share with other users or third parties.
- Provide each minor that submits a report or complaint with a confirmation of receipt of the report or complaint; the process that will be followed when reviewing the report or complaint; an indicative timeframe for deciding the report or complaint; and possible outcomes.

[63] 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.

- Prioritise reports and complaints submitted by minors and provide each minor that has submitted the report or complaint with their reasoned decision without undue delay, in a way that is adapted to the age of the minor. Response times should be appropriate to the issue being reported or complained about.
- 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.

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 has to click through four different links. Once the user arrives in the complaints section, they have to 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

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:

- 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. The support tools should bechild-friendly and accessible (see Section 6.4 on Online interface and other tools) and should connect minors directly with the relevant national support lines, such as those that form part of the national Safer Internet Centres and INHOPE networks.
- Introduce directly visible warning messages, links to relevant national supportlines ([64]) and other authoritative sources when minors search for, upload, generate or share 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 whena

[64] Such as those that form part of the national Safer Internet Centres and INHOPE networks.

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.

- Ensure that if AI features and systems such as AI chatbots and filters are integrated into the service of an online platform, technical measures are implemented to warn minors that they are interacting with an AI system ([65]), that interactions with this system are different from human interactions and that these systems can provide information that is factually inaccurate and can 'hallucinate'. This warning should be easily visible and directly accessible from the interface and throughout the entirety of the minor's interaction with the AI system. For example, AI chatbots should not be displayed in priority or as part of suggested contacts or grouped with users the minor is connected to.

- If the online platform includes 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. No information about the user or their account should be available to any accounts that the user has blocked.

- 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).

- 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,

[65] 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.

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

Tools for guardians are software, features, functionalities, or applications designed to help guardians manage their minor's online activity, privacy, safety and well-being.

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. 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.

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:

- Be easy to use, age-appropriate and not disproportionately restrict minors' rights to privacy or access services, considering the best interest of the minor.
- Apply regardless of the device or operating system used to access the service.
- Provide clear a 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.
- Ensure that changes can only be made with the same degree of authorisation required in the initial activation of the tools.
- Be compatible with the availability of interoperable one-stop-shop tools for guardians gathering all settings and tools.

Such tools may include features such as managing screen time or setting spending limits for the minor, managing account settings, seeing the accounts that the minor communicates with, or other features to supervise uses of the online platforms that may be detrimental to the minor's privacy, safety and security.

Commented [A42]: The guidelines lack the requirement for the online platforms to also verify that the guardian is indeed the person that is legally the guardian of the child in question. This should be added and the Commission should also clarify how online platforms can/should verify this.

Commented [A43]: While we agree that the guidelines should encourage providers to put in place guardian control tools, the guidelines should also take into account paragraph 76 of the UN General comment No. 25 (2021) on children's rights in relation to the digital environment: "*The digital environment presents particular problems for parents and caregivers in respecting children's right to privacy. Technologies that monitor online activities for safety purposes, such as tracking devices and services, if not implemented carefully, may prevent a child from accessing a helpline or searching for sensitive information. States parties should advise children, parents and caregivers and the public on the importance of the child's right to privacy and on how their own practices may threaten that right. They should also be advised about the practices through which they can respect and protect children's privacy in relation to the digital environment, while keeping them safe. Parents' and caregivers' monitoring of a child's digital activity should be proportionate and in accordance with the child's evolving capacities.*"

Commented [A44]: Should a guardian be able to use the guardian control tools even if they themselves do not have an account at the online platform? And if so, how should the online platform deal with that?

Commented [A45]: We consider that more clarity is needed on ''interoperable one-stop-shop tools''.We believe that children must be able to 'object' against the use of a tool by a guardian if such is in the best interest of the child. (For example, when a parent is abusive towards a child, the child should take action against the use of any tools for guardians) This would also be in line with the spirit of article 15(4) GDPR.

8 GOVERNANCE

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)

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:

- 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.
- 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 and users in matters related to minors' privacy, safety and security.
- Fostering a culture of privacy, safety and security for minors on the service. This includes:
    - fostering 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.
    - 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 ([66]).
- 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 ([67]).
- Having procedures to ensure regular monitoring of compliance with Article 28(1) of Regulation (EU) 2022/2065.

[66] 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.

[67] 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.

- Ensuring that any technological and organisational solutions employed to implement these guidelines are 'state-of-the-art' and are aligned with European[68] or national guidance on the protection of minors ([69]) and the highest available standards ([70]).

- Putting in place a process to systematically gather data about the harms and risks to the privacy, safety and security of minors that occur on the platform, and reporting on this data to the provider's senior management body. This is without prejudice to as the providers of VLOPs and VLOSEs obligations stemming from Articles 34 and 35 of Regulation (EU) 2022/2065.

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

Commented [A46]: While it's very welcome that references have been made to guidance published by the EDPB and the DPAs, it will be important to be clear on who has regulatory competence for enforcing these issues.

8.2 Terms and conditions

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.

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 primarily directed at minors or predominantly used by them to explain the conditions for, and any restrictions on, the use of the service in a way that minors can understand([71])([72]).

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

[68] EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default

[69] 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-OnlineSafety-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-ofchildren-and-young-people-on-digital-platforms/; Dutch Ministry of the Interior and Kingdom Relations. (2022). *Code for children's rights*. Available: https://codevoorkinderrechten.nl/wpcontent/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/cnilpublishes-8-recommendations-enhance-protection-children-online; Unabhängiger Beauftragter für Fragen des sexuellen Kindesmissbrauchs. (n.d.). *Rechtsfragen Digitales*. Available: https://beauftragtemissbrauch.de/themen/recht/rechtsfragen-digitales

[70] 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

[71] 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.

[72]

- Include information about:
  - The steps that users need to take from account creation to its deletion.
  - 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.
  - 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.
  - How minors are protected from this content and behaviour.
  - 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.
- Are searchable and easy to find throughout the user's experience on the platform.
- Are upheld and implemented in practice.

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 ([73]).

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.

8.3 Monitoring and evaluation

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:

- 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)

[73] For example, by publishing them in the Digital services terms and conditions database: https://platformcontracts.digital-strategy.ec.europa.eu/

2022/2065. ([74])

- Regularly consulting with minors, guardians and 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.
- 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 to the harms and risks to the privacy, safety and security of minors on their platform.

8.4 Transparency

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.

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. Therefore, it considers that providers of online platforms should make available on an accessible interface on their online platforms and in easy-to-understand language for minors the following information:

- Provide information to minors and, where relevant, their guardians, 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:
  - any age verification or estimation methods used, how these methods work and any third party used to provide any age verification or estimation methods.
  - any measures recommended in the present guidelines and put in place by the provider of the online platform.
  - 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.

Commented [A47]: A reference to Article 13 GDPR, which requires controllers to inform data subjects about a number of elements, including about the types of personal data processed in age assurance mechanisms, would be beneficial.

[74] As indicated in the Introduction of these guidelines (section 1, page 4), 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 and VLOSEs 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.

- 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).
- 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.
- the AI tools, products and features that are incorporated into the platform, their limitations and the potential consequences of their use;
- the registration process where one is offered.
- any tools for guardians that are offered, explaining how to use them, ~~and~~ how they protect minors online,

  and what types of information about the minor's online activity guardians can obtain via the use of such tools.
- how content that breaches the platform's terms and conditions is moderated and the consequences of this moderation.
- how to use the different reporting, complaints, redress and support tools referred to in the present guidelines.
- the online platform's terms and conditions.

- Ensure that this information, all warnings and any other communications recommended in the present guidelines are:
  - child-friendly, age-appropriate, and easily accessible to all minors, including those with disabilities and/or additional accessibility needs.
  - presented clearly in a way that is easy to understand and is as simple and succinct as possible.
  - 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. 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.
  - engaging for minors. This may require the use of graphics, videos, and/or characters or other techniques.
- Any measures and changes implemented to comply with Article 28(1) of Regulation (EU) 2022/2065 could be communicated 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

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. The Commission encourages providers of online platforms accessible to minors, Digital Services Coordinators, 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.

10 ANNEX I, 5 C TYPOLOGY OF RISKS

The OECD ([75]) and researchers ([76]) have classified the risks that minors can encounter online, in order for service providers, 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 ([77])

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

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

[75] 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

[76] 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

[77] 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

consequences to minors' mental health and physical wellbeing, for example content promoting suicide, eating disorders or extreme violence.

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).

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.

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. Consumer risks also include risks related to contracts, for example the sale of users' data or unfair terms and conditions.

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:

- **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.
- **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 of online platforms.
- **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.

Other cross cutting risks ([78]) can also include:

- **Additional safety and security risks** relate to minors' safety, particularly physical safety, as well as all cybersecurity issues.
- **Misuse risks** relate to risks or harms to minors stemming from the misuse of the online platform, or its features.

[78] 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