



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**

## 2           1    INTRODUCTION

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

11   There is, however, wide consensus among policy makers, regulatory authorities, civil  
12   society, researchers, educators and guardians <sup>(2)</sup> that the current level of privacy, safety  
13   and security online of minors is often inadequate. The design and features of online  
14   platforms and the services offered by providers of online platforms accessible to minors  
15   may create risks to minors' privacy, safety and security and exacerbate existing risks.  
16   These risks include, for example, exposure to illegal content <sup>(3)</sup> and harmful content, as  
17   well as unwanted contact that undermines minors' privacy, safety and security or that may  
18   impair the physical or mental development of minors. They also include cyberbullying or  
19   contact from individuals seeking to harm minors, such as those seeking to sexually abuse  
20   or extort minors, human traffickers and those seeking to recruit minors into criminal gangs,  
21   or promote radicalisation and violent extremism. Minors may also face risks related to  
22   extensive use or overuse of online platforms and exposure to inappropriate or exploitative  
23   practices, including in relation to gambling. The increasing integration of artificial  
24   intelligence ("AI") chatbots and companions into online platforms as well as AI driven  
25   deep fakes may also affect how minors interact with online platforms, exacerbate existing  
26   risks, and pose new ones that can negatively affect a minor's privacy, safety and  
27   security <sup>(4)</sup>. These risks can originate from the direct experience of the minor with the  
28   platform and/or from the actions of other users on the platform.

29   These guidelines aim to support providers of online platforms in addressing these risks by  
30   providing a set of measures that the Commission considers will help providers to ensure a  
31   high level of privacy, safety and security on their platforms. For instance, making minors'  
32   accounts more private will, inter alia, help providers of online platforms reduce the risk of  
33   unwanted or unsolicited contact. Implementing age assurance measures <sup>(5)</sup> may, inter alia,  
34   help providers reduce the risk of minors being exposed to services, content, conduct,

---

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

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

<sup>(3)</sup> Illegal content includes but is not limited to content depicting illicit drug trafficking, terrorist and violent extremist content and child sexual abuse material.

<sup>(4)</sup> 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.

<sup>(5)</sup> See section 6.1 on age assurance.

35 contacts or commercial practices that undermine their privacy, safety and security.  
36 Adopting these and other measures – on matters from recommender systems and  
37 governance to user support and reporting – may help providers of online platforms make  
38 online platforms safer, more secure and more privacy preserving for minors.

## 39           2   SCOPE OF THE GUIDELINES

40 It is in the light of the aforementioned risks that the Union legislature enacted Article 28  
41 of Regulation (EU) 2022/2065 of the European Parliament and the Council <sup>(6)</sup>.  
42 Paragraph 1 of that provision obliges providers of online platforms accessible to minors to  
43 put in place appropriate and proportionate measures to ensure a high level of privacy,  
44 safety, and security of minors, on their service. Paragraph 2 prohibits providers of online  
45 platform from presenting advertisements on their interface based on profiling, as defined  
46 in Article 4, point (4), of Regulation (EU) 2016/679, using personal data of the recipient  
47 of the service when they are aware with reasonable certainty that the recipient of the service  
48 is a minor. Paragraph 3 specifies that compliance with the obligations set out in Article 28  
49 shall not oblige providers of online platforms accessible to minors to process additional  
50 personal data in order to assess whether the recipient of the service is a minor. Paragraph  
51 4 provides that the Commission, after consulting the Board, may issue guidelines to assist  
52 providers of online platforms in the application of paragraph 1.

53 These guidelines describe the measures that the Commission considers that providers of  
54 online platforms accessible to minors should take to ensure a high level of privacy, safety  
55 and security for minors online, in accordance with Article 28(1) of Regulation (EU)  
56 2022/2065 of the Council and the Parliament. The obligation laid down in that provision  
57 is addressed to providers of online platforms whose services are accessible to minors <sup>(7)</sup>.  
58 Recital 71 of that Regulation explains that “[a]n online platform can be considered  
59 accessible to minors when its terms and conditions permit minors to use the service, when  
60 its service is directed at or predominantly used by minors, or where the provider is  
61 otherwise aware that some of the recipients of its service are minors”.

62 As regards the first scenario described in that recital, the Commission considers that a  
63 provider of an online platform that simply declares in its terms and conditions that it is not  
64 accessible to minors but does not put any effective measure in place to avoid that minors  
65 access its service, cannot claim that its online platform falls outside the scope of Article  
66 28(1) of Regulation (EU) 2022/2065 for that simple reason. For example, providers of  
67 online platforms that host and disseminate adult content, such as online platforms  
68 disseminating pornographic content , and therefore restrict, in their terms and conditions,

---

<sup>(6)</sup> 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.

<sup>(7)</sup> 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.

69 the use of their service to users over the age of 18 year, will nevertheless be considered  
70 accessible to minors within the meaning of Article 28(1) of Regulation (EU) 2022/2065  
71 where users under the age of 18 in fact access their service.

72 As regards the third scenario, recital 71 of Regulation (EU) 2022/2065 explains that one  
73 example of a situation in which a provider of online platform should be aware that some  
74 of the recipients of its service are minors is where that provider already processes the  
75 personal data of those recipients revealing their age for other purposes, and this reveals  
76 that some of those recipients are minors. Other examples of situations in which a provider  
77 may be aware that some of the recipients of its online platform service are minors include  
78 those in which the online platform is known to appeal to minors, the provider of the online  
79 platform offers similar services to those used by minors, the online platform is promoted  
80 to minors and where the provider of the online platform has conducted or commissioned  
81 research that identifies minors as recipients of its service.

82 Pursuant to Article 19 of Regulation (EU) 2022/2065, the obligation laid down in Article  
83 28(1) of Regulation (EU) 2022/2065 does not apply to providers of online platforms that  
84 qualify as micro or small enterprises, except where their online platform has been  
85 designated by the Commission as a very large online platform in accordance with Article  
86 33(4) of that Regulation <sup>(8)</sup>.

87 Other provisions of Regulation (EU) 2022/2065 are also aimed at ensuring the protection  
88 of minors online <sup>(9)</sup>. These include, inter alia, several provisions in Section 5 of Chapter  
89 III of Regulation (EU) 2022/2065, which imposes additional obligations on providers of  
90 very large online platforms (“VLOPs”) and very large online search engines (“VLOSEs”)  
91 <sup>(10)</sup>. To the extent that the obligations expressed in those provisions also relate to the  
92 privacy, safety and security of minors within the meaning of Article 28(1) of Regulation  
93 (EU) 2022/2065, these guidelines build on these provisions. These guidelines do not aim  
94 to interpret those provisions and providers of VLOPs and VLOSEs should not expect that  
95 adopting the measures described below, either partially or in full, suffices to ensure  
96 compliance with their obligations under Section 5 of Chapter III of Regulation (EU)  
97 2022/2065, as those providers may need to put in place additional measures which are not

---

<sup>(8)</sup> 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,

<sup>(9)</sup> 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.

<sup>(10)</sup> 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.

98 set out in these guidelines and which are necessary for them to comply with the obligations  
99 stemming from those provisions <sup>(11)</sup>.

100 Article 28(1) of Regulation (EU) 2022/2065 should also be seen in the light of other Union  
101 legislation and non-binding instruments which aim to address the risks to which minors  
102 are exposed online <sup>(12)</sup>. Those instruments also contribute to achieving the objective of  
103 ensuring a high level of privacy, safety and security of minors online, and thus complement  
104 the application of Article 28(1) of Regulation (EU) 2022/2065. These guidelines should  
105 not be understood as interpreting those instruments.

106 While these guidelines set out measures that ensure a high level of privacy, safety and  
107 security for minors online, providers of online platforms are encouraged to adopt those  
108 measures for the purposes of protecting all users, and not just minors. Creating a privacy  
109 preserving, safe and secure online environment for everyone contributes to privacy, safety  
110 and security online of minors.

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

114 By adopting these guidelines, the Commission indicates that it will apply these guidelines  
115 to the cases described therein and thus that it imposes a limit on the exercise of its  
116 discretion whenever applying Article 28(1) of Regulation (EU) 2022/2065. As such, these  
117 guidelines may therefore be considered a significant and meaningful benchmark on which  
118 the Commission will base itself when applying Article 28(1) of Regulation (EU)  
119 2022/2065 and determining the compliance of providers of online platforms accessible to  
120 minors with that provision. Nevertheless, adopting and implementing measures set out in  
121 these guidelines, either partially or in full, shall not automatically entail compliance with  
122 that provision.

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

---

<sup>(11)</sup> 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.

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

127

### 3 STRUCTURE OF THE GUIDELINES

128 Section 4 of these guidelines sets out the general principles which should govern all  
129 measures that providers of online platforms accessible to minors put in place to ensure a  
130 high level of privacy, safety, and security of minors on their service. Sections 5 to 8 of  
131 these guidelines set out the main measures that the Commission considers that such  
132 providers should put in place to ensure such a high level of privacy, safety and security.  
133 These include Risk review (section 5), Service design (section 6), Reporting, user support  
134 and tools for guardians (section 7) and Governance (section 8).

135 The measures described in Sections 5 to 8 of these guidelines are not exhaustive. Other  
136 measures may also be deemed appropriate and proportionate to ensure a high level of  
137 privacy, safety and security for minors in accordance with Article 28(1) of Regulation (EU)  
138 2022/2065, such as those measures resulting from compliance with other pieces of EU  
139 legislation or adherence to national guidance on the protection of minors <sup>(13)</sup> or technical  
140 standards <sup>(14)</sup>. In addition, new measures may be identified in the future that enable  
141 providers of online platforms accessible to minors to better comply with their obligation  
142 to ensure a high level of privacy, safety and security of minors on their service.

143

### 4 GENERAL PRINCIPLES

144 The Commission considers that any measure that a provider of an online platform  
145 accessible to minors puts in place to comply with Article 28(1) of Regulation (EU)  
146 2022/2065 should adhere to the following general principles:

- 147 • **Proportionality:** Article 28(1) of Regulation (EU) 2022/2065 requires any  
148 measure taken to comply with that provision to be appropriate and proportionate to  
149 ensure a high level of privacy, safety, and security of minors. Since different online  
150 platforms may pose different types of risks for minors, it will not always be  
151 proportionate for all providers of online platforms to apply all the measures  
152 described in these guidelines. Determining whether a particular measure is  
153 proportionate will require a case-by-case review by each provider (i) of the risks to  
154 minors' privacy, safety and security stemming from its online platform, considering  
155 *inter alia* the type of service it provides and its nature, its intended or current use,  
156 and the user base of the service, and (ii) of the impact of the measure on children's  
157 rights and other rights and freedoms enshrined in the Charter of Fundamental  
158 Rights of the European Union ("the Charter") (see Section 5 on Risk review).
- 159 • **Children's rights:** These rights are enshrined in the Charter and the United Nations  
160 Convention on the Rights of the Child ("the UNCRC"), to which all Member States

---

<sup>(13)</sup> This includes for example the Directives and Regulations cited in footnote 12, the forthcoming guidelines by the European Data Protection Board (EDPB) on processing of minor personal data in accordance with Regulation (EU) 2016/679 (GDPR).

<sup>(14)</sup> 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](https://www.oecd.org/en/publications/children-in-the-digital-environment_9b8f222e-en.html)

161 are parties <sup>(15)</sup>. Children’s rights form an integral part of human rights and all those  
162 rights are interrelated, interdependent and indivisible. Therefore, to ensure that  
163 measures to achieve a high level of privacy, safety and security for minors on an  
164 online platform are appropriate and proportionate, it is necessary to consider all  
165 children’s rights, including their right to protection, non-  
166 discrimination, inclusion, participation, privacy, information and freedom of  
167 expression, among others.

168 • **Privacy-, safety- and security-by-design:** providers of online platforms  
169 accessible to minors should integrate the highest standards of privacy, safety and  
170 security in the design, development and operation of their services <sup>(16)</sup>.

171 • **Age-appropriate design:** providers of online platforms accessible to minors  
172 should design their services to align with the developmental, cognitive, and  
173 emotional needs of minors, while ensuring their safety, privacy, and security <sup>(17)</sup>.

## 174 5 RISK REVIEW

175 Where a provider of an online platform accessible to minors is determining which  
176 measures are appropriate and proportionate to ensure a high level of safety, privacy and  
177 security to minors on their platform, the Commission considers that that provider should,  
178 at a minimum, identify:

- 179 • How likely it is that minors will access its service.
- 180 • The risks to the privacy, safety and security of minors that the online platform may  
181 pose or give rise to, based on the 5Cs typology of risks (Annex I). This includes an  
182 examination of how different aspects of the platform may give rise to these risks.  
183 For example, aspects such as the purpose of the platform, its design, interface, value  
184 proposition, marketing, features, functionalities, number and type of users and uses  
185 (actual and expected) may all be relevant.

---

<sup>(15)</sup> These rights are elaborated by the United Nations Committee on the Rights of the Child as regards the digital environment in their General Comments No. 25. Office of the High Commissioner for Human Rights. (2021). General Comment No. 25 (2021) on children's rights in relation to the digital environment. Available: <https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation>

<sup>(16)</sup> According to Article 25 GDPR, operators processing minors’ personal data must already implement appropriate organisational and technical measures to protect the rights of data subject (data protection by design and default). This obligation is enforced by the competent data protection authorities in line with Article 51 GDPR. See EDPB guidelines 4/2019 on Article 25 Data Protection by Design and by Default. Available: [https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and\\_en](https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en)

<sup>(17)</sup> 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/wp-content/uploads/2022/02/Code-voor-Kinderrechten-EN.pdf>

- 186 • The measures that the provider is already taking to prevent and mitigate these risks.
  - 187 • Any additional measures that are identified in the review as appropriate and
  - 188 proportionate to ensure a high level of privacy, safety and security for minors on
  - 189 their service.
  - 190 • The potential positive and negative effects on children’s rights of any measure that
  - 191 the provider currently has in place and any additional measures, ensuring that these
  - 192 rights are not disproportionately or unduly restricted. Children’s rights that may be
  - 193 adversely affected by some measures include, for example, children’s rights to
  - 194 participation, freedom of expression and information. This is relevant when
  - 195 determining the proportionality of measures.
- 196 When conducting this review, providers of online platforms accessible to minors should
- 197 be guided by the best interest of the minor <sup>(18)</sup>.
- 198 Providers should carry out the review whenever they make significant changes to their
- 199 online platform and should consider publishing its outcomes.
- 200 Existing tools to carry out child rights impact assessments can support providers in
- 201 carrying out this review <sup>(19)</sup>. The Commission may issue additional guidance or tools to
- 202 support providers in carrying out the review, including through specific tools for child
- 203 rights impact assessments.
- 204 For providers of VLOPs and VLOSEs this risk review should be carried as part of the
- 205 general assessment of systemic risks under Article 34 of Regulation (EU) 2022/2065,
- 206 which oftentimes will complement and go beyond the risk assessment pursued in
- 207 accordance with the present guidelines.

## 208 **6 SERVICE DESIGN**

### 209 **6.1 Age assurance**

#### 210 **6.1.1 Introduction and terminology**

211 The Commission considers measures restricting access based on the recipient’s age to be

212 an effective means to ensure a high level of privacy, safety and security for minors on

213 online platforms, where those measures are used to protect minors from accessing age-

214 inappropriate content online, such as gambling services or pornography, or from being

215 exposed to risks such as grooming.

---

<sup>(18)</sup> 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.

<sup>(19)</sup> Dutch Ministry of the Interior and Kingdom Relations (BZK). (2024). *Child Rights Impact Assessment (Fillable Form)*. Available: <https://www.nldigitalgovernment.nl/document/childrens-rights-impact-assessment-fill-in-document/>; 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>

216 Such measures are commonly referred to as “age assurance”<sup>(20)</sup>. The most common age  
217 assurance measures currently available and applied by online platforms fall into three  
218 broad categories: self-declaration, age estimation, and age verification.

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

222 • **Age estimation** consists of independent methods which allow a provider to establish  
223 that a user is likely to be of a certain age, to fall within a certain age range, or to be over  
224 or under a certain age<sup>(21)</sup>.

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

227 The main difference between age estimation and age verification measures is the level of  
228 accuracy. Whereas age verification provides certainty about the age of the user in principle  
229 down to the day, age estimation provides an approximation of the user’s age.

## 230 **6.1.2 Determining whether to put in place age assurance measures**

231 Before deciding whether to put in place any age assurance method, providers of online  
232 platforms accessible to minors should always conduct an assessment to determine whether  
233 such a method is appropriate to ensure a high level of privacy, safety and security for  
234 minors on their service and whether it is proportionate, or whether such a high level may  
235 be achieved already by relying on other less far-reaching measures<sup>(22)</sup>. In this regard, the  
236 Commission is of the view that providers should also consider other measures set out in  
237 other sections of these guidelines as an alternative to age assurance measures.

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

240 Online platforms might have only some content, sections or functions that pose a risk to  
241 minors or may have parts of their platform where the risk can be mitigated by other  
242 measures and parts where it cannot. In these cases, providers of online platforms should  
243 assess which content, sections or functions on their platform carry risks for minors and  
244 implement an age assurance method as proximate to these as possible.

245 5

---

(20) 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>

(21) *ibid*; CEN-CENELEC. (2023). *Workshop Agreement 18016 Age Appropriate Digital Services Framework*: [https://www.cencenelec.eu/media/CEN-CENELEC/CWAs/ICT/cwa18016\\_2023.pdf](https://www.cencenelec.eu/media/CEN-CENELEC/CWAs/ICT/cwa18016_2023.pdf).

(22) 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.

246 **6.1.3 Determining which age assurance methods to use**

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

- 250 • Where applicable Union or national law prescribes a minimum age to access certain  
251 products or services offered and/or displayed in any way on the online platform,  
252 such as by way of example:
  - 253 ○ the sale of alcohol,
  - 254 ○ access to pornographic content,
  - 255 ○ or access to gambling content.
- 256 • Where the terms and conditions or any other contractual obligations of the service  
257 require a user to be 18 years or older to access the service, due to identified risks to  
258 minors, even if there is no formal age requirement established by law.
- 259 • 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  
262 measures <sup>(23)</sup>.

263 Methods that rely on verified and trusted government-issued IDs may constitute an  
264 effective age verification method. Member States are currently in the process of providing  
265 each of their citizens, residents and businesses an EU Digital Identity Wallet, <sup>(24)</sup> which  
266 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.

267

268 To facilitate age verification before the EU Digital Identity Wallet becomes available, the  
269 Commission is currently working on an EU age verification solution as a standalone age  
270 verification measure. Once finalized, the EU age verification solution will aim to provide  
271 a valid example and a benchmark for a device-based method of age verification.

272

---

<sup>(23)</sup> These risks can be identified via the review of risks set out in Section 5.

<sup>(24)</sup> As provided for under Section 1 of Chapter II of Regulation (EU) No 910/2014, as amended by Regulation (EU) 2024/1183

### 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.

273

274 While providers of online platforms accessible to minors may use other age verification  
275 methods to ensure a high level of privacy, safety, and security of minors, those methods  
276 should ensure an equivalent level of verification as the EU age verification application.

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

- 280 • Where the terms and conditions or similar contractual obligations of the service  
281 require a user to be above a required minimum age that is lower than 18 to access  
282 the service, indicating the provider's assessment of when the online platform is safe  
283 and secure for minors to use <sup>(25)</sup> <sup>(26)</sup>.
- 284 • Where the provider of the online platform has identified at least medium risks to  
285 minors on their platform as established in its risk review (see Section 5 on Risk  
286 Review) <sup>(27)</sup> and those risks cannot be mitigated by less restrictive measures. The  
287 Commission considers this will be the case where the risk is not high enough to  
288 require age verification but not low enough that it would be appropriate to have no  
289 age assurance methods in place at all.

---

<sup>(25)</sup> 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.

<sup>(26)</sup> In some cases, it may be possible for the provider to verify that the minor was signed up by their guardians.

<sup>(27)</sup> These risks can be identified via the review of risks set out in Section 5.

290 Providers of online platforms accessible to minors that are confronted with those two  
 291 scenarios may also opt to put in place age verification methods instead. In any event,  
 292 providers should conduct a proportionality assessment justifying the adoption of age  
 293 assurance measures prior to putting them in place.

294 When considering age assurance methods that require the processing of personal data,  
 295 providers of online platforms accessible to minors should take into account the European  
 296 Data Protection Board (EDPB) statement on Age Assurance <sup>(28)</sup>.

297

Recommended measure	Scenarios
<b>Age verification only</b>	<ul style="list-style-type: none"> <li>• 18+ restricted content and goods, such as pornography and gambling platforms</li> <li>• Services designed for an adult audience only, such as adults dating platforms, posing risks to minors</li> <li>• Terms and conditions and/or any other contractual obligations requiring minimum age of 18</li> <li>• High risk services where only AV would protect minors, as established in the risk review (see Section 5 on Risk Review)</li> </ul>
<b>Age estimation or age verification</b>	<ul style="list-style-type: none"> <li>• 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 to use for minors above the indicated age</li> <li>• Medium risk services - age assurance is used to ensure age-appropriate experiences for minors online</li> </ul>

**Good practice**

MegaBetting <sup>(29)</sup> 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.

298

299

<sup>(28)</sup> See EDPB statement 1/2025 on Age Assurance. Available: [https://www.edpb.europa.eu/system/files/2025-04/edpb\\_statement\\_20250211ageassurance\\_v1-2\\_en.pdf](https://www.edpb.europa.eu/system/files/2025-04/edpb_statement_20250211ageassurance_v1-2_en.pdf)

<sup>(29)</sup> All good and poor practice examples in these guidelines refer to fictitious 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  $\pm 2$  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.

300 Where a platform has determined that age assurance is necessary to achieve a high level  
301 of privacy, safety and security for minors on their service, it should always make more  
302 than one age assurance method available. This will help to avoid the exclusion of users  
303 who, despite being eligible to access an online platform, cannot avail themselves of a  
304 specific age assurance method. Where age verification or estimation is appropriate and  
305 proportionate, at least two different age verification or estimation methods, or one  
306 verification and one estimation method, should be provided <sup>(30)</sup>. Furthermore, providers of  
307 online platforms should provide a redress mechanism for users to complain about any  
308 incorrect age assessments by the provider <sup>(31)</sup>.

**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.

309

310 **6.1.4 Assessing the effectiveness of any age assurance method**

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

- 314
  - **Accuracy.** How accurately any given method determines the age of the user.

---

<sup>(30)</sup> See also point 17 of the EDPB Statement on age assurance.

<sup>(31)</sup> 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.

315 The accuracy of an age verification or estimation method should be assessed against  
316 appropriate metrics to evaluate the extent to which it can correctly determine the  
317 age or age range of a person <sup>(32)</sup>. Providers of online platforms should periodically  
318 review whether the technical accuracy of the method used still matches the state-  
319 of-the-art.

320 • **Reliability.** How reliable a given method works in practice in real-world  
321 circumstances.

322 For a method to be reliable, it should be available continuously at any time, and  
323 work in different real-world circumstances, beyond ideal lab conditions. Providers  
324 of online platforms accessible to minors should assess, before employing a specific  
325 age assurance solution, that any data relied upon as part of the age assurance process  
326 comes from a reliable source. For example, a self-signed proof of age would not be  
327 considered reliable.

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

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

336 • **Non-Intrusiveness.** How intrusive is a given method on users’ rights.

337 Providers of online platforms accessible to minors should assess the impact the  
338 chosen method will have on recipients' rights and freedoms, including their right to  
339 privacy, data protection and freedom of expression <sup>(33)</sup>. According to the European  
340 Data Protection Board, and in line with Article 28(3) of regulation 2022/2065 <sup>(34)</sup>,  
341 a provider should only process the age-related attributes that are strictly necessary  
342 for the specific purpose and should not provide additional means for providers to  
343 identify, locate, profile or track natural persons <sup>(35)</sup>. If the method is more intrusive  
344 than another method that provides the same level of assurance and effectiveness,  
345 the less intrusive method should be chosen. This includes an assessment of the  
346 extent to which the method provides transparency about the process and/or puts  
347 information about the user at risk.

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

---

<sup>(32)</sup> 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.

<sup>(33)</sup> 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.

<sup>(34)</sup> 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.

<sup>(35)</sup> See EDPB statement 1/2026 on Age Assurance point 2.3 and 2.4.

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

352 The Commission considers that **self-declaration** <sup>(36)</sup> does not meet all the requirements  
353 above, in particular the requirement for robustness and accuracy. Therefore, it does not  
354 consider self-declaration to be an appropriate age assurance method to ensure a high level  
355 of privacy, safety, and security of minors in accordance with Article 28(1) of Regulation  
356 (EU) 2022/2065.

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

## 363 **6.2 Registration**

364 Registration or authentication may influence whether and how minors are able to access a  
365 given service in a safe, age-appropriate and rights-preserving way. Where registration is  
366 required or offered as a possibility to access an online platform accessible to minors, the  
367 Commission considers that the provider of that platform should:

- 368 • Explain to users the benefits of registration or why registration is necessary.
- 369 • Ensure that the registration process is easy for all minors to access and navigate,  
370 including those with disabilities or additional accessibility needs.
- 371 • Ensure that the registration process includes measures to help users understand  
372 whether they are allowed to use the service and measures to reduce the risk of them  
373 making further attempts to register if they are below the minimum age required by  
374 the online platform accessible to minors <sup>(37)</sup>.
- 375 • Avoid encouraging or enticing users who are below the minimum age required by  
376 the online platform accessible to minors to create accounts.
- 377 • Ensure that it is easy for minors to log out and to have their profile deleted at their  
378 request.

---

<sup>(36)</sup> 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>

<sup>(37)</sup> This is without prejudice to additional requirements stemming from other laws, such as Article 12 of Regulation (EU) 2016/679.

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

## 382 6.3 Account settings

### 383 6.3.1 Default settings

384 Default settings are an important tool that providers of online platforms accessible to  
385 minors may use to mitigate risks to minors’ privacy, safety and security, such as the risk  
386 of unwanted contact by individuals seeking to harm minors. Evidence suggests that minors  
387 tend not to change their default settings, which means that the default settings remain for  
388 most users and thus become crucial in driving behaviour <sup>(38)</sup>.

389 The Commission therefore considers that providers of online platforms accessible to  
390 minors that use default settings to ensure a high level of privacy, safety, and security of  
391 minors on their service for the purposes Article 28(1) of Regulation (EU) 2022/2065  
392 should:

- 393 • Ensure that privacy, safety and security by design principles are consistently applied to  
394 all account settings for minors.
- 395 • Set accounts for minors to the highest level of privacy, safety and security by default.  
396 This includes designing **default settings** in such a way as to ensure that:
- 397 ○ accounts of minors only allow interaction such as likes, tags, comments, direct  
398 messages, reposts and mentions by accounts they have previously accepted as  
399 “friends” or contacts. This categorisation requires regular review.
  - 400 ○ No account, except the minor’s, can download or take screenshots of content  
401 uploaded or shared by the minor to the platform.
  - 402 ○ only accounts that the minor has previously accepted as contacts can see their  
403 content and posts.
  - 404 ○ geolocation, microphone and camera, contact synchronisation as well as all  
405 optional tracking features are turned off.
  - 406 ○ the default autoplay of videos and hosting live streams are turned off.
  - 407 ○ push notifications are turned off by default and are always off during core sleep  
408 hours, adapting the core sleep hours to the age of the minor. When push  
409 notifications are actively enabled by the user, they should only notify the user

---

<sup>(38)</sup> 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](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.

410 about interactions arising from the user’s direct contacts and content from  
411 accounts or channels that the user actively follows or engages with (for example,  
412 push notifications should never be inauthentic and always mentions precisely the  
413 user or creator the notification comes from).

414 ○ features that may contribute to excessive use, such as the number of “likes” or  
415 “reactions”, communication “streaks”, the “... is typing” function, ephemeral  
416 content, and “read receipts,” are turned off.

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

422 ○ filters that can have detrimental effects on body image, self-esteem and mental  
423 health are turned off.

424 ● Regularly test and update default settings, ensuring that they remain effective against  
425 emerging online risks and trends, including any risks to minors’ privacy, safety and  
426 security identified by the provider in the course of their review of risks (see Section 5  
427 on Risk review).

428 ● Ensure that users’ choices about settings remain effective after updates or changes to  
429 their service.

430 ● Ensure that minors are not in any way encouraged or enticed to change their settings to  
431 lower levels of privacy, safety and security.

432 ● Ensure that minors are provided with incremental degrees of control over their settings,  
433 according to their age and needs. <sup>(39)</sup>

434 ● Ensure that settings are explained to minors in a child-friendly and accessible way (see  
435 Section 6.46.46.46.46.4 on Online interface and other tools).

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

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

442 ● Actively and continuously raise awareness and seek agreement from minors and ask for  
443 their choices to be reaffirmed or modified at certain points.

---

<sup>(39)</sup> Minors experience different developmental stages and have different levels of maturity and understanding at different ages. This is recognised *inter alia* in the UN Committee on the Rights of the Child General Comment No. 25 on children’s rights in relation to the digital environment 2021, para. 19-21. A practical table on ages and developmental stages is available, *inter alia* as Annex to the *Dutch Children’s Code*. Available at: <https://codevoorkinderrechten.nl/wp-content/uploads/2022/02/Code-voor-Kinderrechten-EN.pdf>

- 444 • Present age-appropriate warning signals clearly explaining the potential consequences  
445 of any changes.
- 446 • Automatically turn off geolocation, microphone and camera as well as optional tracking  
447 features after the session ends, if a minor turns them on.

### 448 **6.3.2 Availability of settings, features and functionalities**

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

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

468 When assessing whether any additional settings, features or functionalities should be  
469 removed from minors' accounts altogether to ensure a high level of privacy, safety and  
470 security of minors, the Commission considers that providers of online platforms accessible  
471 to minors should assess the risks that those settings and functionalities may present to the  
472 privacy, safety and security of minors on their platform.

### 473 **6.4 Online interface design and other tools**

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

477 Without prejudice to the obligations of providers of VLOPs and VLOSEs under Section 5  
478 of Chapter III of Regulation (EU) 2022/2065 and independently of the providers of online  
479 platforms' obligations as regards the design, organisation and operation of their online  
480 interfaces deriving from Article 25 that Regulation, the Commission considers that  
481 providers of online platforms accessible to minors should adopt and implement

482 functionalities allowing minors to decide how to engage with their services. This could  
483 include, for example:

- 484 • Ensuring that minors are not exposed to persuasive design features that are aimed  
485 predominantly at engagement or that may lead to extensive use or overuse of the  
486 platform or the forming of problematic or compulsive behavioural habits. This  
487 includes the possibility to scroll indefinitely, the superfluous requirement to  
488 perform a specific action to receive updated information on an application,  
489 automatic triggering of video content, notifications artificially timed to regain  
490 minors' attention, notifications that are artificial, including those that pretend to be  
491 another user or social notifications about content that the user has never engaged  
492 with, signs communicating scarcity <sup>(40)</sup>, and the creation of virtual rewards for  
493 performing repeated actions on the platform.
- 494 • Introducing customisable, easy-to-use, child-friendly and effective time  
495 management tools (see Section 6.4 on Online interface design and other tools) to  
496 increase minors' awareness of their time spent on online platforms and help them  
497 engage with the service for no longer than they or their guardians intend. In order  
498 to be effective, these tools should create real frictions so that minors are effectively  
499 deterred from spending more time on the platform. These could also include nudges  
500 that favour safer options.
- 501 • Ensuring that any tools, features, functionalities, settings, prompts, options and  
502 reporting, feedback and complaints mechanisms that are recommended in the  
503 present guidelines are child-friendly, age-appropriate, easy to find, access,  
504 understand and use for all minors, including those with disabilities and/or  
505 additional accessibility needs, and are easy to use and understand, and engaging,  
506 and do not require changing devices to complete any action involved.

**Poor practice**

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

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

---

<sup>(40)</sup> 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.

## 508 **6.5 Recommender systems and search features**

509 Recommender systems determine the manner in which information is prioritised and  
 510 presented to minors. As a result, such systems have an important impact on whether and  
 511 to what extent minors encounter certain types of content, contacts or conducts online.  
 512 Recommender systems may pose and exacerbate risks to minors' privacy, safety and  
 513 security online by, for example, amplifying content that can have a negative impact on  
 514 minors' safety and security <sup>(41)</sup>.

515 The Commission recalls the obligations for all providers of all categories of online  
 516 platform concerning recommender system transparency under Article 27 of Regulation  
 517 (EU) 2022/2065 and the additional requirements for providers of VLOPs and VLOSEs  
 518 under Articles 34 (1), 35(1), and 38 of Regulation (EU) 2022/2065 in this respect <sup>(42)</sup>.

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

### 523 **6.5.1 Testing and adaptation of the design and functioning of recommender** 524 **systems for minors**

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

- 527 • Take into account specific needs, characteristics, disabilities and additional  
 528 accessibility needs of minors when defining the objectives, parameters and  
 529 evaluation strategies of recommender systems, in particular by not only optimising

---

<sup>(41)</sup> Munn, L. (2020). Angry by design: Toxic communication and technical architectures. *Humanities and Social Sciences Communications*, 7(53). Available: <https://doi.org/10.1057/s41599-020-00550-7>; Milli, S. et al. (2025). Engagement, user satisfaction, and the amplification of divisive content on social media. *PNAS Nexus*, 4(3) pgaf062. Available: <https://doi.org/10.1093/pnasnexus/pgaf062>; Piccardi, T. et al. (2024). Social Media Algorithms Can Shape Affective Polarization via Exposure to Antidemocratic Attitudes and Partisan Animosity. Available: [10.48550/arXiv.2411.14652](https://arxiv.org/abs/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>

<sup>(42)</sup> 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 remit, which contribute to a high level of privacy, safety and protection of fundamental rights online.

- 530 or predominantly maximising time spent on, engagement and interaction with the  
531 platform. Parameters and metrics related to accuracy, diversity, inclusivity and  
532 fairness should also be considered.
- 533 • Ensure that recommender systems promote minors’ access to information that is  
534 relevant and adequate for them, with due consideration to their age group.
  - 535 • Ensure that recommender systems do not rely on the on-going collection of  
536 behavioural data that captures all or most of the minor's activities on the platform,  
537 such as watch time and click through rates, and do not rely on the collection of any  
538 behavioural data that captures the user's activities off the platform.
  - 539 • Prioritise ‘explicit user-provided signals’ over ‘implicit engagement-based signals’  
540 to determine the content displayed and recommended to minors. The selection of  
541 such signals should be justified in the best interest of the minor, which will help to  
542 ensure that they contribute to a high level of safety and security for minors. For the  
543 purposes of the present guidelines, ‘explicit user-provided signals’ shall be  
544 understood as referring to user feedback and interactions that indicate users’  
545 explicit preferences, both positive and negative, including the stated and  
546 deliberative selection of topics of interest, surveys, reporting <sup>(43)</sup>, and other quality-  
547 based signals. For the purposes of the present guidelines, ‘implicit engagement-  
548 based signals’ shall be understood as referring to ambiguous signals that infer user  
549 preferences from their activities (browsing behaviour on a platform), such as time  
550 spent viewing content and click-through rates.
  - 551 • Implement measures to prevent a minor’s repeated exposure to content that could  
552 pose a risk to minors’ safety and security, particularly when encountered  
553 repeatedly, such as content promoting unrealistic beauty standards or dieting,  
554 content that glorifies or trivialises mental health issues, such as anxiety or  
555 depression, discriminatory content, illegal content and distressing content depicting  
556 violence or encouraging minors to engage in dangerous activities.
  - 557 • Put in place measures to reduce the risk that content is recommended which poses  
558 risks to minors’ privacy, safety or security, or that has been reported or flagged by  
559 users, trusted flaggers or other actors or content moderation tools, and whose  
560 lawfulness and adherence to the platforms’ terms and conditions have not yet been  
561 verified (see Section 6.7 on Moderation for more information).
  - 562 • Implement measures to ensure that recommender systems do not enable or facilitate  
563 the dissemination of illegal content or the commitment of criminal offences against  
564 minors.

---

<sup>(43)</sup> 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.

- 565 • Ensure that minors’ search results and suggestions for contacts prioritise accounts  
566 whose identity has been verified and contacts connected to the network of the  
567 minor, or contacts in the same age range as the minor.
- 568 • Ensure that search features, including but not limited to text autocomplete on the  
569 search bar and suggested terms and key phrases, do not recommend content that  
570 qualifies as harmful to the privacy, safety or security of minors, for instance by  
571 blocking search terms that are well-known to trigger content that is deemed to be  
572 harmful to minors’ privacy, safety and/or security, such as particular words, slang,  
573 hashtags or emojis <sup>(44)</sup>.

574

## 575 **6.5.2 User control and empowerment**

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

- 579 • Provide minors with the opportunity to reset their recommended feeds  
580 completely and permanently.
- 581 • Provide prompts for the minor to search for new content after a certain amount  
582 of interaction with the recommender system.
- 583 • Ensure that minors can choose an option of their recommender system that is  
584 not based on profiling.
- 585 • Ensure that relevant reporting and feedback mechanisms set out in Section 7.1  
586 of the present guidelines have a swift, direct and lasting impact on the  
587 parameters, editing and output of the recommender systems. This includes  
588 permanently removing reported content and contacts from recommendations  
589 (including content reported for hiding) and reducing the visibility of similar  
590 content and accounts.

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

- 594 • Explain why each specific piece of content was recommended to them, including  
595 information about the parameters used and the user signals collected for that  
596 specific recommendation. Providers should also provide information to minors  
597 about prompts that encourage minors to search for new content after a certain  
598 period of time interacting with the recommender system. This information  
599 should be child-friendly and accessible (see Section 8.4 on Transparency).
- 600 • Ensure that any settings and information provided to minors about their  
601 recommender systems are presented in child-friendly and accessible ways (see

---

<sup>(44)</sup> 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.

602 Sections 6.4 on Online interface design and other tools and Section 8.4 on  
603 Transparency for more details).

- 604 • Offer minors the options to modify or influence the parameters of their  
605 recommender systems by for example allowing them to select content categories  
606 and activities they are most or least interested in. This should be offered during  
607 the account creation process and throughout the user’s time on the platform.  
608 These preferences should directly influence the recommendations provided by  
609 the system, ensuring that they align more closely with the minor’s age and best  
610 interests <sup>(45)</sup>.

611

## 612 **6.6 Commercial practices**

613 Minors are particularly exposed to the persuasive effects of commercial practices and have  
614 a right to be protected against economically exploitative practices <sup>(46)</sup>. Despite this, minors  
615 are confronted with commercial practices everywhere online, facing diverse, dynamic and  
616 personalised persuasive tactics through, for example, advertisement, product placements,  
617 the use of in-app currencies, influencer marketing or AI-enhanced nudging <sup>(47)</sup>. This can  
618 have a negative effect on minors’ privacy, safety and security when using the services of  
619 an online platform.

620 In line with, and without prejudice to, the existing horizontal legal framework<sup>(48)</sup> and the  
621 more specific rules in Regulation (EU) 2022/2065 on advertising (Articles 26 and 28(2))  
622 or dark patterns (Article 25), the Commission considers that providers of online platforms  
623 accessible to minors should adopt the following measures to ensure a high level of privacy,  
624 safety, and security of minors, on their service for the purposes Article 28(1) of Regulation  
625 (EU) 2022/2065:

---

<sup>(45)</sup> See Articles 27(1) and (3) of Regulation (EU) 2022/2065.

<sup>(46)</sup> 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>

<sup>(47)</sup> 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>

<sup>(48)</sup> 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 17<sup>th</sup> November 2025, on the way that this Regulation interacts with other legal acts, in particular the acts referred to above.

- 626 • Ensure that minors’ lack of commercial literacy is not exploited by considering  
627 minors’ age, vulnerabilities and limited capacity to engage critically with  
628 commercial practices on the platform and provide relevant support.
- 629 • Have a responsible marketing and advertising policy in place that does not allow  
630 harmful, unethical and unlawful advertising <sup>(49)</sup> to, for or by minors. This entails  
631 considering the appropriateness of advertising campaigns for different age groups,  
632 addressing their adverse impact, and taking adequate security measures to protect  
633 minors as well as to ensure that they have access to information that is in their best  
634 interest.
- 635 • Ensure that declarations of commercial communication are clearly visible, child-  
636 friendly and accessible (see Section 8.4 on Transparency) and consistently used  
637 throughout the service, for instance with the use of an icon or a similar sign to  
638 clearly indicate that content is advertising. These should be regularly tested and  
639 reviewed in consultation with minors, their guardians and other relevant  
640 stakeholders.
- 641 • Ensure that minors are not exposed to marketing and communication of products  
642 or services that can have an adverse impact on their privacy, safety and security,  
643 including as identified in the provider’s risk review (see Section 5 on Risk review).
- 644 • Ensure that minors are not exposed to hidden or disguised advertising, whether  
645 placed by the provider of the online platform or the users of the service <sup>(50)</sup>. In this  
646 context, the Commission recalls that providers of online platforms are also obliged,  
647 under Article 26(2) of Regulation (EU) 2022/2065, to provide recipients of the  
648 service with a functionality to declare whether the content they provide is or  
649 contains commercial communications <sup>(51)</sup>. Examples of disguised commercial  
650 communications include, but are not limited to, product placements by influencers,  
651 product showcases and other forms of subtle promotion that may deceive or  
652 manipulate minors into purchasing products or services.
- 653 • Ensure transparency of economic transactions in an age-appropriate way and avoid  
654 the use of intermediate virtual currencies, such as tokens or coins, that can be  
655 exchanged with real money and then used to buy other virtual items, which can  
656 have the effect of reducing transparency of economic transactions and may be  
657 misleading for minors.

---

<sup>(49)</sup> 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.

<sup>(50)</sup> 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.

<sup>(51)</sup> 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.

- 658 • Ensure that minors, when accessing online platforms or parts and features thereof  
659 that are presented or appear as being free <sup>(52)</sup>, are not exposed to in-app or in-game  
660 purchases that are or appear to be necessary to access or use the service.
- 661 • Ensure that minors are not exposed to practices that can lead to excessive or  
662 unwanted spending or addictive behaviours, by ensuring that virtual items such as  
663 loot boxes, other products with random or unpredictable outcomes or gambling-  
664 like features are not accessible to minors, and by introducing separation or friction  
665 between content and the purchasing of related products.
- 666 • Ensure that minors are not exposed to manipulative design techniques <sup>(53)</sup>, such as  
667 scarcity <sup>(54)</sup>, intermittent or random rewards, or persuasive design techniques, <sup>(55)</sup>.
- 668 • Ensure that minors are not exposed to unwanted purchases, e.g. by considering  
669 deploying effective tools for guardians (see Section 7.3 on Tools for guardians).

## 670 **6.7 Moderation**

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

674 The Commission recalls the obligations related to terms and conditions set out in Article  
675 14 of Regulation (EU) 2022/2065 and to transparency reporting provided in Article 15 of  
676 that Regulation for providers of intermediary services, which includes providers of online  
677 platforms; and the obligations related to trusted flaggers <sup>(56)</sup> for providers of online  
678 platforms set out in Article 22 of that Regulation. It also recalls the 2025 Code of Conduct  
679 on Countering Illegal Hate Speech Online +, which constitutes a code of conduct within  
680 the meaning of Article 45 of Regulation (EU) 2022/2065. In addition to those obligations,  
681 the Commission considers that providers of online platforms accessible to minors should

---

<sup>(52)</sup> 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.

<sup>(53)</sup> As set out in Article 25 of Regulation (EU) 2022/2065.

<sup>(54)</sup> 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

<sup>(55)</sup> 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.

<sup>(56)</sup> 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.

682 put in place the following measures to ensure a high level of privacy, safety, and security  
683 of minors on their service for the purposes Article 28(1) of Regulation (EU) 2022/2065:

684 • Define clearly and transparently what the platform considers as content and  
685 behaviour that is harmful for minors' privacy, safety and security, ideally in  
686 cooperation with independent experts and civil society. This should include any  
687 content and behaviour that is illegal under EU or national law. Providers of online  
688 platforms accessible to minors should always ensure that their terms and conditions  
689 clearly define harmful content and behaviour and do not unduly restrict any rights  
690 of minors, including minors' right to freedom of expression and information.

691 • Establish moderation policies and procedures that set out how content and  
692 behaviour that is harmful for the privacy, safety and security of minors is detected  
693 and how it will be moderated and ensure that these policies and/or procedures are  
694 enforced in practice.

695 • Take into account the following factors when prioritising moderation: the  
696 likelihood of the content causing harm to a minor's privacy, safety and/or security,  
697 the impact of the harm on that minor, and the number of minors who may be  
698 harmed.

699 • Consider human review for content that substantially exceeds the average number  
700 of views and for any reported accounts that the provider suspects may pose a risk  
701 of harm to minors' privacy, safety or security.

702 • Put in place effective technologies, internal mechanisms and preventative features  
703 to reduce the risk of content and behaviour that are harmful to minors' privacy,  
704 safety of security from being shown to minors in their accounts' interface or other  
705 functionalities of the service, including:

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

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

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

**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.

717

## 718 **7 REPORTING, USER SUPPORT AND TOOLS FOR GUARDIANS**

### 719 **7.1 User reporting, feedback and complaints**

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

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

728 In addition to those obligations, the Commission considers that providers of online  
729 platforms accessible to minors should put in place the following measures to ensure a high  
730 level of privacy, safety, and security of minors on their service for the purposes Article  
731 28(1) of Regulation (EU) 2022/2065:

- 732 • Implement reporting, feedback and complaints mechanisms that:
  - 733 ○ are effective, child-friendly and accessible (see Section 6.4 on Online  
734 interface design and other tools)
  - 735 ○ Allow minors to report content, activities, individuals, accounts, or groups  
736 they believe may violate the platform's terms and conditions. This includes  
737 any content, user or activity that is considered by the platform to be harmful  
738 to minors' privacy, safety, and/or security (see Section 5 on Risk review).
  - 739 ○ Allow all users to report content, activities, individuals, accounts, or groups  
740 that they deem inappropriate or undesirable for minors, or where they are  
741 uncomfortable with the idea of such content, activities, individuals accounts  
742 or groups being accessible to minors.
  - 743 ○ Allow all users to report a suspected underage account, where a minimum  
744 age is stated in the platform's terms and conditions.
  - 745 ○ Allow minors to provide feedback about all content, activities, individuals,  
746 accounts or groups that they are shown on their accounts and that make  
747 them feel uncomfortable or that they want to see more or less of. These  
748 options could include phrases such as "Show me less/more", "I don't want  
749 to see/I am not interested in", "I don't want to see content from this  
750 account," "This makes me feel uncomfortable," "Hide this," "I don't like  
751 this," or "This is not for me". Providers of online platforms should ensure  
752 that these options are designed in such a way that they are only visible to  
753 the user, so that they cannot be misused by others to bully or harass minors

- 754 on the platform. Providers of online platforms should adapt their  
755 recommender systems in response to this feedback <sup>(57)</sup>.
- 756 ○ Where the provider uses age assurance methods, allow any user to access  
757 an effective internal complaint-handling system that enables them to lodge  
758 complaints, electronically and free of charge, against an assessment by the  
759 provider of the user’s age. This complaint handling system should fulfil the  
760 conditions set out in Article 20 of Regulation (EU) 2022/2065.
- 761 • Ensure that the reporting, feedback and complaints mechanisms established under  
762 Article 20 of Regulation (EU) 2022/2065 <sup>(58)</sup>:
- 763 ○ Contribute to a high level of privacy, safety and security for minors.
- 764 ○ Are aligned with fundamental rights, in particular children’s rights.
- 765 ○ Are available for intuitive and immediate access for all minors, including  
766 for those with disabilities and/or additional accessibility needs.
- 767 ○ Are easy for minors to use and understand, are age-appropriate and  
768 engaging (see Section 6.4 on Online interface design and other tools).  
769 Providers could, for example, state that reporting is confidential and useful  
770 for users.
- 771 ○ Are available for non-registered users if they may access the online  
772 platform’s content.
- 773 • If reporting categories are used, ensure that they are adapted to the youngest users  
774 allowed on the platform. Complex menu systems should be avoided. There should  
775 also be an option available that allows minors to provide their own reasons for a  
776 report.
- 777 • Provide minors with easy access to information about whether the provider of the  
778 online platform discloses reports and/or complaints to other users. Where providers  
779 of online platforms share information with others, they should explain to minors  
780 when, how and what information related to reports and/or complaints they share  
781 with other users or third parties.
- 782 • Provide each minor that submits a report or complaint with a confirmation of  
783 receipt of the report or complaint; the process that will be followed when reviewing

---

<sup>(57)</sup> See section 6.5 of the present guidelines for information about how this information should affect the provider’s recommender systems.

<sup>(58)</sup> 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.

784 the report or complaint; an indicative timeframe for deciding the report or  
785 complaint; and possible outcomes.

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

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

795

#### **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.

796

## **7.2 User support measures**

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

802 • Have clear, easily identifiable and accessible support tools that allow minors to  
803 seek help when encountering suspicious, illegal or inappropriate content, accounts  
804 or behaviour that make them feel uncomfortable. The support tools should be child-  
805 friendly and accessible (see Section 6.4 on Online interface and other tools) and  
806 should connect minors directly with the relevant national support lines, such as  
807 those that form part of the national Safer Internet Centres and INHOPE networks.

808 • Introduce directly visible warning messages, links to relevant national support lines  
809 <sup>(59)</sup> and other authoritative sources when minors search for, upload, generate or  
810 share content that is potentially illegal or harmful for the privacy, safety and  
811 security of minors (as explained in the section 6.7 on Moderation). Providers of  
812 online platforms should also refer minors to relevant national support lines when a

---

<sup>(59)</sup> Such as those that form part of the national Safer Internet Centres and INHOPE networks.

813 minor submits a report related to such content. The referral should be made  
814 immediately after the provider of the online platform becomes aware of the activity  
815 or the minor submits a report.

816 • Ensure that if AI features and systems such as AI chatbots and filters are integrated  
817 into the service of an online platform, technical measures are implemented to warn  
818 minors that they are interacting with an AI system <sup>(60)</sup>, that interactions with this  
819 system are different from human interactions and that these systems can provide  
820 information that is factually inaccurate and can ‘hallucinate’. This warning should  
821 be easily visible and directly accessible from the interface and throughout the  
822 entirety of the minor’s interaction with the AI system. For example, AI chatbots  
823 should not be displayed in priority or as part of suggested contacts or grouped with  
824 users the minor is connected to.

825 • If the online platform includes functionalities related to user connection, posting  
826 content or user communication, provide minors with the option to anonymously  
827 block or mute any other user or account, including those that are not connected to  
828 them. No information about the user or their account should be available to any  
829 accounts that the user has blocked.

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

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

**Good practice**

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

839

---

<sup>(60)</sup> 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.

840 **7.3 Tools for guardians**

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

843 The Commission considers that tools for guardians should be treated as complementary to  
844 safety by design and default measures and to any other measures put in place to comply  
845 with Article 28(1) of Regulation (EU) 2022/2065, including those described in these  
846 guidelines. Tools for guardians should not be used as the sole measure to ensure a high  
847 level of privacy, safety and security of minors on online platforms, nor be used to *replace*  
848 any other measures put in place for that purpose. Nevertheless, the Commission notes that,  
849 when used in combination with other measures, they may contribute to such a high level.

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

- 853 • Be easy to use, age-appropriate and not disproportionately restrict minors’ rights to  
854 privacy or access services, considering the best interest of the minor.
- 855 • Apply regardless of the device or operating system used to access the service.
- 856 • Provide clear a notification to minors of their activation by guardians and put other  
857 safeguards in place considering their potential misuse by guardians such as, for  
858 example, providing a clear sign to the minor in real time when any monitoring  
859 functionality is activated.
- 860 • Ensure that changes can only be made with the same degree of authorisation  
861 required in the initial activation of the tools.
- 862 • Be compatible with the availability of interoperable one-stop-shop tools for  
863 guardians gathering all settings and tools.

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

868 **8 GOVERNANCE**

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

872 **8.1 Governance (general)**

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

- 877 • Implementing internal policies that outline how the provider of the online platform  
878 seeks to ensure a high level of privacy, safety and security for minors on its service.
- 879 • Assigning to a dedicated person or team the responsibility for ensuring a high level  
880 of minors' privacy, safety and security. This person or team should have sufficient  
881 resources as well as sufficient authority to have direct access to the senior  
882 management body of the provider of the online platform and should also be a  
883 central point of contact for regulators and users in matters related to minors'  
884 privacy, safety and security.
- 885 • Fostering a culture of privacy, safety and security for minors on the service. This  
886 includes:
- 887     ○ fostering a culture of child participation in the design and functioning of the  
888 platform. This should be done in safe, ethical, inclusive and meaningful  
889 ways, in children's best interests, and should provide for feedback  
890 mechanisms to explain to minors how their views have been taken into  
891 account.
- 892     ○ raising awareness of how the provider upholds children's rights on its  
893 platform and the risks that minors on the platform may face to their privacy,  
894 safety and/or security <sup>(61)</sup>.
- 895 • Providing persons responsible for minors' privacy, safety and security, developers,  
896 persons in charge of moderation and/or those receiving reports or complaints from  
897 minors, with relevant training and information <sup>(62)</sup>.
- 898 • Having procedures to ensure regular monitoring of compliance with Article 28(1)  
899 of Regulation (EU) 2022/2065.

---

<sup>(61)</sup> 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, established in each Member State, demonstrate the value of awareness-raising efforts in preventing and responding to online harms and risks.

<sup>(62)</sup> 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.

- 900 • Ensuring that any technological and organisational solutions employed to  
901 implement these guidelines are ‘state-of-the-art’ and are aligned with national  
902 guidance on the protection of minors <sup>(63)</sup> and the highest available standards <sup>(64)</sup>.
- 903 • Putting in place a process to systematically gather data about the harms and risks  
904 to the privacy, safety and security of minors that occur on the platform, and  
905 reporting on this data to the provider’s senior management body. This is without  
906 prejudice to as the providers of VLOPs and VLOSEs obligations stemming from  
907 Articles 34 and 35 of Regulation (EU) 2022/2065.
- 908 • Exchanging between platforms and providers, as well as with Digital Services  
909 Coordinators, trusted flaggers, civil society organisations and other relevant  
910 stakeholders, good practices and technological solutions that are aimed at ensuring  
911 a high level of privacy, safety and security for minors.

## 912 **8.2 Terms and conditions**

913 Terms and conditions provide a framework for governing the relationship between the  
914 provider of the online platform and its users. They set out the rules and expectations for  
915 online behaviour and play an important role in establishing a safe, secure and privacy  
916 respecting environment.

917 The Commission recalls the obligations for all providers of intermediary services as  
918 regards terms and conditions set out in Article 14 of Regulation (EU) 2022/2065, which  
919 includes the obligation for providers of intermediary services primarily directed at minors

---

<sup>(63)</sup> 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](https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf); Coimisiún na Meán. (2024). *Online safety code*. Available: <https://www.cnam.ie/app/uploads/2024/11/Coimisiun-na-Mean-Online-Safety-Code.pdf>; IMY (Swedish Authority for Privacy Protection). (2021). *The rights of children and young people on digital platforms*. Available: <https://www.imy.se/en/publications/the-rights-of-children-and-young-people-on-digital-platforms/>; Dutch Ministry of the Interior and Kingdom Relations. (2022). *Code for children's rights*. Available: <https://codevoorkinderrechten.nl/wp-content/uploads/2022/02/Code-voor-Kinderrechten-EN.pdf>; CNIL. (2021). *CNIL publishes 8 recommendations to enhance protection of children online*. Available: <https://www.cnil.fr/en/cnil-publishes-8-recommendations-enhance-protection-children-online>; Unabhängiger Beauftragter für Fragen des sexuellen Kindesmissbrauchs. (n.d.). *Rechtsfragen Digitales*. Available: <https://beauftragte-missbrauch.de/themen/recht/rechtsfragen-digitales>

<sup>(64)</sup> 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](https://www.oecd.org/en/publications/children-in-the-digital-environment_9b8f222e-en.html)

920 or predominantly used by them to explain the conditions for, and any restrictions on, the  
921 use of the service in a way that minors can understand <sup>(65)</sup> <sup>(66)</sup>.

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

- 924 • Include information about:
- 925 ○ The steps that users need to take from account creation to its deletion.
  - 926 ○ Community guidelines that promote a positive, safe and inclusive  
927 atmosphere and that explain what conduct is expected and prohibited on  
928 their service, and what the consequences of non-compliance are.
  - 929 ○ The types of content and behaviour that are considered to be harmful for  
930 minors’ privacy, safety and/or security. This includes but is not limited to  
931 illegal content that is harmful for minors’ privacy, safety and/or security and  
932 the dissemination of this content.
  - 933 ○ How minors are protected from this content and behaviour.
  - 934 ○ The tools that are used to prevent, mitigate and moderate content, conduct  
935 and features that are illegal or harmful for the privacy, safety and security of  
936 minors, and the complaints process.
- 937 • Are searchable and easy to find throughout the user’s experience on the platform.
- 938 • Are upheld and implemented in practice.

939 In addition, the Commission considers that the providers of online platforms accessible to  
940 minors should ensure changes to the terms and conditions are logged and published <sup>(67)</sup>.

**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.

---

<sup>(65)</sup> 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.

<sup>(66)</sup> As indicated in the Introduction of these guidelines, certain provisions of Regulation (EU) 2022/2065 including points (5) and (6) of article 14, impose additional obligations on providers of very large online platforms (“VLOPs”). To the extent that the obligations expressed therein also relate to the privacy, safety and security of minors within the meaning of Article 28(1), the present guidelines build on these provisions.

<sup>(67)</sup> For example, by publishing them in the Digital services terms and conditions database: <https://platform-contracts.digital-strategy.ec.europa.eu/>

941

### 942 **8.3 Monitoring and evaluation**

943 The Commission considers that providers of online platforms accessible to minors should  
944 adopt effective monitoring and evaluation practices to ensure a high level of privacy, safety  
945 and security for minors on their service for the purposes Article 28(1) of Regulation (EU)  
946 2022/2065. This includes, but is not limited to:

- 947 • Regularly monitoring and evaluating the effectiveness of any elements of the  
948 platform that concern the privacy, safety and security of minors on the platform.  
949 This includes, for example, the platform’s online interface, systems, settings, tools,  
950 functionalities and features and reporting, feedback and complaints mechanisms,  
951 and measures taken to comply with Article 28(1) of Regulation (EU)  
952 2022/2065. <sup>(68)</sup>
- 953 • Regularly consulting with minors, guardians and relevant stakeholders on the  
954 design and evaluation of any elements of the platform that concern the privacy,  
955 safety and security of minors on the platform. This should include testing these  
956 elements with minors and taking their feedback into account. To contribute to non-  
957 discrimination and accessibility, providers should, where possible, involve in these  
958 consultations minors from a diverse range of cultural and linguistic backgrounds,  
959 of different ages, with disabilities and/or additional accessibility needs.
- 960 • Adjusting the design and functioning of the aforementioned elements based on the  
961 results of these consultations and on technical developments, research, changes in  
962 user behaviour or policy, product and usage evolutions, and changes to the harms  
963 and risks to the privacy, safety and security of minors on their platform.

964

### 965 **8.4 Transparency**

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

970 The Commission considers that providers of online platforms accessible to minors should  
971 make all necessary and relevant information on the functioning of their services easily  
972 accessible for minors to ensure a high level of privacy, safety and security on their services.  
973 Therefore, it considers that providers of online platforms should make available on an

---

<sup>(68)</sup> 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.

974 accessible interface on their online platforms and in easy-to-understand language for  
975 minors the following information:

976 • Provide information to minors and, where relevant, their guardians, about any  
977 measures put in place to ensure a high level of privacy, safety or security of minors  
978 on the platform. This includes information about:

979 ○ any age verification or estimation methods used, how these methods work  
980 and any third party used to provide any age verification or estimation  
981 methods.

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

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

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

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

992 ○ the AI tools, products and features that are incorporated into the platform,  
993 their limitations and the potential consequences of their use;

994 ○ the registration process where one is offered.

995 ○ any tools for guardians that are offered, explaining how to use them and  
996 how they protect minors online.

997 ○ how content that breaches the platform’s terms and conditions is moderated  
998 and the consequences of this moderation.

999 ○ how to use the different reporting, complaints, redress and support tools  
1000 referred to in the present guidelines.

1001 ○ the online platform’s terms and conditions.

1002 • Ensure that this information, all warnings and any other communications  
1003 recommended in the present guidelines are:

1004 ○ child-friendly, age-appropriate, and easily accessible to all minors,  
1005 including those with disabilities and/or additional accessibility needs.

1006 ○ presented clearly in a way that is easy to understand and is as simple and  
1007 succinct as possible.

1008 ○ presented to the minor in ways that are easy to review and that provide for  
1009 immediate and intuitive access, at the points at which they become relevant.  
1010 For example, where the terms and conditions refer to a specific feature, the  
1011 key information about this feature is presented when the minor engages  
1012 with it.

- 1013                   ○ engaging for minors. This may require the use of graphics, videos, and/or  
1014                   characters or other techniques.
- 1015                   • Any measures and changes implemented to comply with Article 28(1) of  
1016                   Regulation (EU) 2022/2065 could be communicated internally and made public to  
1017                   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.

## 1018                   **9 REVIEW**

1019                   These guidelines constitute a first interpretation by the Commission of Article 28(1) of  
1020                   Regulation (EU) 2022/2065. The Commission will review these guidelines as soon as this  
1021                   is necessary in view of practical experience gained in the application of that provision and  
1022                   the pace of technological, societal, and regulatory developments in this area. The  
1023                   Commission encourages providers of online platforms accessible to minors, Digital  
1024                   Services Coordinators, the research community and civil society organisations to  
1025                   contribute to this process. Following such a review, the Commission may, in consultation  
1026                   with the European Board for Digital Services, decide to amend these guidelines.

1027

**10 ANNEX I, 5 C TYPOLOGY OF RISKS**

1028 The OECD <sup>(69)</sup> and researchers <sup>(70)</sup> have classified the risks that minors can encounter  
 1029 online, in order for service providers, academia and policy makers to better understand and  
 1030 analyse them. This classification of risks is known as the 5Cs typology. It helps in  
 1031 identifying risks and includes 5 categories of risks: content, conduct, contact, consumer  
 1032 risks, cross-cutting risks. These risks may manifest when there are no appropriate and  
 1033 proportionate measures in place to ensure a high level of privacy, safety and security,  
 1034 causing potential infringement of a number of children’s rights.

1035 **5C typology of risks <sup>(71)</sup>**

Risks for children in the digital environment				
Risk categories	Content	Conduct	Contact	Consumer
<b>Cross-cutting risks</b>	<b>Additional privacy, safety and security risks</b> <b>Advanced technology risks</b> <b>Risks on health and wellbeing</b> <b>Misuse risks</b>			
<b>Risk manifestation</b>	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

1036

1037 **Content risks:** Minors can be unexpectedly and unintentionally exposed to content that  
 1038 potentially harms them: a. hateful content, b. harmful content c. illegal content; d.  
 1039 disinformation. These types of contents are widely considered to have serious negative  
 1040 consequences to minors’ mental health and physical wellbeing, for example content  
 1041 promoting suicide, eating disorders or extreme violence.

1042 **Conduct risks:** Refer to behaviours minors may actively adopt online, and which can pose  
 1043 risks to both themselves and others such as a. hateful behaviour (e.g., minors  
 1044 posting/sending hateful content/messages e.g. cyberbullying); b. harmful behaviour (e.g.,  
 1045 minors posting/sending violent or pornographic content); c. illegal behaviour (e.g., minors

<sup>(69)</sup> 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](https://www.oecd.org/en/publications/children-in-the-digital-environment_9b8f222e-en.html)

<sup>(70)</sup> 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/ssor.71817>

<sup>(71)</sup> 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](https://www.oecd.org/en/publications/children-in-the-digital-environment_9b8f222e-en.html)

1046 posting/sending child sexual abuse material or terroristic content); and d. user-generated  
1047 problematic behaviour (e.g., participation in dangerous challenges; sexting).

1048 **Contact risks:** Refer to situations in which minors are victims of the interactions, as  
1049 opposed to the actor: a. hateful encounters, b. harmful encounters (e.g. the encounter takes  
1050 place with the intention to harm the minor), c. illegal encounters (e.g. can be prosecuted  
1051 under criminal law), and d. other problematic encounters. Examples of contact risks  
1052 include, but are not limited to online grooming, online sexual coercion and extortion,  
1053 sexual abuse via webcam, cyberbullying and sex trafficking. These risks also extend to  
1054 online fraud practices such as phishing, marketplace fraud, and identity theft.

1055 **Consumer risks:** Minors can also face risks as consumers in the digital economy: a.  
1056 marketing risks (e.g. loot boxes, advergames.), b. commercial profiling risks (e.g. product  
1057 placement or receiving advertisements intended for adults such as dating services), c.  
1058 financial risks (e.g. fraud or spending large amounts of money on without the knowledge  
1059 or consent of their guardians), d. security risks. Consumer risks also include risks related  
1060 to contracts, for example the sale of users' data or unfair terms and conditions.

1061 **Cross cutting risks:** These are risks that cut across all risk categories and are considered  
1062 highly problematic as they may significantly affect minors' lives in multiple ways. They  
1063 are:

- 1064 • **Advanced technology risks** involve minors encountering new dangers as technology  
1065 develops, such as AI chatbots that might provide harmful information or be used for  
1066 grooming by exploiting vulnerabilities or the use of biometric technologies that can  
1067 lead to abuse, identity fraud, lead to exclusion etc.
- 1068 • **Health and wellbeing risks** include potential harm to minors' mental, emotional, or  
1069 physical well-being. For example, increased obesity/anorexia and mental health issues  
1070 linked to the use of online platforms.
- 1071 • **Additional privacy and data protection risks** stem from access to information about  
1072 minors and the danger of geolocation features that predators could exploit to locate and  
1073 approach minors.

1074 Other cross cutting risks <sup>(72)</sup> can also include:

- 1075 • **Additional safety and security risks** relate to minors' safety, particularly physical  
1076 safety, as well as all cybersecurity issues.
- 1077 • **Misuse risks** relate to risks or harms to minors stemming from the misuse of the  
1078 online platform, or its features.

---

<sup>(72)</sup> 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/ss0ar.71817>