Council of the European Union

Brussels, 18 September 2026
(OR. en)

13321/26
ADD 1

Interinstitutional File:
2026/0286 (COD)

AUDIO 106
TELECOM 435
COMPET 1094
JEUN 213
MI 907
DIGIT 236
CONSOM 266
DATAPROTECT 289
JAI 1178
DISINFO 63
CT 109
ENT 230
CES 18
CDR 205
CODEC 1709

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	17 September 2026
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	SWD(2026) 681 final
Subject:	COMMISSION STAFF WORKING DOCUMENT Analysis of impacts Accompanying the document Proposal for a Regulation of the European Parliament and of the Council EU KIDS ACT - 'EU Keeping Internet Digital Spaces Accountable and Trustworthy'

Delegations will find attached document SWD(2026) 681 final.

Encl.: SWD(2026) 681 final

EUROPEAN
COMMISSION

Brussels, 17.9.2026
SWD(2026) 681 final

COMMISSION STAFF WORKING DOCUMENT

Analysis of impacts

Accompanying the document

Proposal for a Regulation of the European Parliament and of the Council

EU KIDS ACT - 'EU Keeping Internet Digital Spaces Accountable and Trustworthy'

{COM(2026) 681 final}

Table of contents

1. INTRODUCTION: POLITICAL AND LEGAL CONTEXT 3
   1.1. Context 3
   1.2. The European regulatory framework 5
   1.3. Existing and supporting evidence 8
2. STATE OF PLAY AND PROBLEM STATEMENT: THE PROTECTION OF MINORS IN THE EUROPEAN UNION 14
   2.1. A fragmented internal market 14
   2.2. An insufficient level of protection for minors online 18
   2.3. A lack of clear requirements for age assurance and ineffective implementation 29
3. PROPOSED REGULATION: A HARMONISED APPROACH TO CHILDREN'S ONLINE SAFETY 33
   3.1. The need for a harmonised European approach 34
   3.2. A regulation for child online safety 34
   3.3. A comprehensive regulatory framework for the protection of minors online. 43
4. IMPACTS: A SAFER ONLINE ENVIRONMENT FOR CHILDREN 45
   4.1. Public health 45
   4.2. Fundamental Rights 55
   4.3. Economic Impacts 63
5. CONCLUSION 81

Glossary

Term or acronym	Meaning or definition
AI	Artificial Intelligence
AI Act	Artificial Intelligence Act
AVMSD	Audiovisual Media Services Directive
BIK+	Better Internet for Kids Strategy
DFA	Digital Fairness Act
DMA	Digital Markets Act
DSA	Digital Services Act
EDPB	European Data Protection Board
EPRS	European Parliamentary Research Service
GDPR	General Data Protection Regulation
OS	Operating System
SICs	Safer Internet Centres
TFEU	Treaty on the Functioning of the European Union
TRIS	EU-level Technical Regulation Information System
VLOPs	Very Large Online Platforms
VLOSEs	Very Large Online Search Engines
VSPs	Video-sharing platform services

1. INTRODUCTION: POLITICAL AND LEGAL CONTEXT

1.1. Context

The digital world has become an essential part of the daily lives of children, influencing their social life, development, education and the way they consume and access entertainment and information.

Globally, both the negative impact of the online world on children, as well as the opportunities it represents, has been the subject of increased attention and scrutiny. In December 2025, Australia became the first country to implement legislation delaying access to social media until the age of 16 ([1]) with further duty of care obligations now under consideration. The UK ([2]) and Brazil ([3]) have dedicated comprehensive risk-based legal and policy frameworks to protect minors online with the UK also considering delaying access to social media ([4]). Canada ([5]), Japan ([6]), Indonesia ([7]) and others are considering comparable approaches ([8]). In the United States, the topic has gained increasing attention at both federal and state level ([9]), with recent litigation shifting towards new liability risks for platform providers ([10]). More recently, the G7 Leaders endorsed principles to strengthen the protection of children online ([11]).

The European Union has made protecting minors online one of its main priorities and is at the forefront of efforts to ensure a safe and empowering online environment for children. Recognising that the protection of mental health of children online is one of the greatest challenges of this decade ([12]), Commission President Ursula von der Leyen announced the establishment of a panel of specialists to advise her on the best approach for Europe on child

[1] Australia Online Safety Amendment (Social Media Minimum Age) Act 2024 (No.127, 2024).
[2] The UK's Online Safety Act 2023 (c. 50).
[3] Brazil's Estatuto Digital da Criança e do Adolescente (Law No. 15.211/2025).
[4] UK's Department for Science, Innovation and Technology, Growing Up in the Online World: A National Consultation, last updated 7 August 2026, https://www.gov.uk/government/consultations/growing-up-in-the-online-world-a-national-consultation. [UK National consultation]
[5] The Government of Canada introduced Bill C-34, the Safe Social Media Act, which would enact two new Acts: The Digital Safety Act and the Digital Safety Commission of Canada Act. The Bill is at an early stage of the legislative process.
[6] Children and Families Agency (Japan), 'Study Group on the Internet Environment for Children' (30th Meeting), Reference Material 3, International Trends in Measures to Protect Children Online, 8 August 2025, https://www.cfa.go.jp/assets/contents/node/basic_page/field_ref_resources/7ce4fa4b-f167-4913-970e-d2fb48108e32/3a0b20c0/20250808_councils_internet-kaigi_30.pdf
[7] Indonesia, Ministry of Communication and Digital Affairs, Ministerial Regulation No. 9 of 2026 on the Implementing Regulation of Government Regulation No. 17 of 2025 on the Governance of Electronic System Operation in Child Protection, 6 March 2026. [Regulation No. 9]
[8] For more information, see Tech Policy Press, Global Social Media Age Restriction Tracker, last updated 22 July 2026, https://social-media-age-tracker.onrender.com/#status=implemented.
[9] At state level, in addition to long-standing laws (Children's Online Privacy Protection Act), more recently, 'The Take it Down Act' entered into force on May 19, 2026. Several proposals are pending in the US Congress and at State level at least 25 states have enacted some sort of age assurance laws.
[10] Thousands of ongoing cases relating to youth online safety, including more than 100 state Attorney General actions, primarily targeting VLOPs and VLOSEs. Most of the legal developments have been driven by a product liability perspective, with cases grounded in consumer law. See for instance: People of the State of California, et al. v. Meta Platforms, Inc., et al., MDL No. 3047, Case Nos. 4:22-md-03047-YGR 4:23-cv-05448-YGR.
[11] G7, Leaders' Call on a Safer Digital Space for Minors, Evian, 17 June 2026, https://www.consilium.europa.eu/media/32fnosbz/leader-s-call-on-a-safer-digital-space-for-minors.pdf.
[12] Von der Leyen, U., 'Europe's choice: Political Guidelines for the next European Commission 2024-2029', July 2024, https://commission.europa.eu/document/e6cd4328-673c-4e7a-8683-f63ffb2cf648_en.

safety online in her 2025 State of the Union address ([13]). The panel brought together specialists from diverse fields including the medical profession, child psychology, computer science, child rights, data protection and consumer rights, as well as youth and parents' representatives.

Following a series of meetings that took place in the first half of 2026, the Co-Chairs of the Special Panel on child online safety, Prof. Dr. Jörg M. Fegert and Dr. Maria Melchior, presented the Report in July 2026. Based on 6 guiding principles, including a developmental approach, equality and diversity, protection of minors, accountability of digital services and consumer rights, empowerment and media education and children's rights and participation, the Report sets out recommendation to improve child safety online. In particular, it recommends EU-wide access restrictions to social media and other digital services, including AI companions, below age 13, harmonised safety by design rules for social media, other digital service and certain artificial intelligence ('AI') systems accessible to minors and proportionate, privacy-preserving age assurance systems ([14]).

The European Parliament has also called for strengthening the protection of children online. In its resolution of November 2025, the European Parliament called for a harmonised European digital age limit of 16 years for access to social media, video-sharing platforms and AI companions, and of 13 years for access to social media with parental consent ([15]). The resolution highlights the importance of age-appropriate design and safety by design and by default to ensure a safe online environment for minors, calling on the Commission to propose legislation ([16]). Further, the European Parliament also notes the existing national fragmentation around age assurance and calls for a European approach providing legal certainty ([17]).

Member States have also prioritised this topic and have called for strengthening protections. Upon the initiative of the Danish presidency, 25 Member States signed the Jutland Declaration in October 2025 calling for a safer online environment, including via age-appropriate design and safety by design and by default and effective and privacy-preserving age verification on social media and other relevant digital services that pose a significant risk for minors ([18]). In its conclusions of October 2025 and of March 2026, the European Council also stressed the importance of protecting minors online, including through a digital age of majority ([19]). At national level, Member States are considering adopting age restrictions for access to certain digital services with France adopting its legislation in Parliament in July 2026. In 2026, France, Greece, Norway, Poland, Austria and Belgium notified their draft legislation via the EU-level Technical Regulation Information System (TRIS) under the Single Market Transparency Directive [20], while several other Member States are currently undergoing consultation processes, discussing drafts within their national parliaments or announcing upcoming

[13] Von der Leyen, U., 'State of the Union 2025', September 2025, https://commission.europa.eu/strategy-and-policy/state-union/state-union-2025_en.
[14] Fegert, J.M. and Melchior, M., *Child Safety Online: protecting and empowering minors in a digital world*, July 2026, https://commission.europa.eu/topics/digital-economy-and-society/special-panel_en. [Fegert and Melchior]
[15] European Parliament resolution of 26 November 2025 on the protection of minors online (2025/2060(INI)) (C/2026/1708) §28.
[16] *Ibid* §36.
[17] *Ibid* §15 and 17.
[18] Danish Presidency of the Council of the European Union, *The Jutland Declaration: Shaping a Safe Online Worlds for Minors*, October 2025.
[19] European Council, 'Conclusions 19 March 2026', EUCO 1/26, 19 March 2026; European Council, 'Conclusions 23 October 2025', EUCO 18/25, 23 October 2025.
[20] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification) (OJ L 241, 17.9.2015, ELI: http://data.europa.eu/eli/dir/2015/1535/oj).

legislative measures. If, within three months of the notification by the Member State, the Commission finds that a notified draft national law concerns a matter covered by a proposal presented by the Commission, Member State shall postpone the adoption of the draft national law to 12 months from the date of notification ([21]).

This call for action at Member State level is supported by children, parents and the public, who are similarly asking for stronger measures to protect children online. 92% of Europeans consider the need to further strengthen children and young people's protection online a top policy priority ([22]). In particular, 54% of parents and 45% of 13-18 years old consider age delays to be an effective solution ([23]). Children and stakeholders also emphasise the responsibility of platforms in providing age-appropriate services. At the Safer Internet Forum in December 2025, the 200 participants, including children, young people and representatives from civil society, highlighted the need for requirements for safety by design, including age-appropriate defaults, recommender systems and interface design. During its meeting in December 2025, the President Youth Advisory Board also pointed to the need to address addictive design and algorithmic systems ([24]).

1.2. The European regulatory framework

As recognised by the Report of the Co-Chairs of the Special Panel, the European Union has set up a 'powerful legislative framework' for the protection of minors online while identifying areas that require further measures ([25]). At its centre, the Digital Services Act (DSA) requires providers of online platforms to ensure a high level of privacy, safety and security on their platforms ([26]). In July 2025, the Commission adopted its guidelines on the protection of minors setting out a benchmark for compliance and outlining measures platforms should take to ensure a high level of privacy, safety and security, which is required by Art. 28 DSA ([27]). The DSA also prohibits advertisements based on profiling for minors ([28]). As part of their risk assessments and mitigation obligations, providers of Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) must also identify, assess and mitigate any systemic risks to the rights of the child, the protection of minors and the protection of mental and physical wellbeing ([29]). In relation to the protection of minors, the Commission has opened 10 formal proceedings against VLOPs and VLOSEs ([30]). In the first half of 2026, the Commission notably

---

[21] Directive (EU) 2015/153 of the European Parliament and the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on information society services (OJ L 241, 17.9.2015, ELI: http://data.europa.eu/eli/dir/2015/1535/oj), Article 6(4).

[22] European Commission, 'Special Eurobarometer on the digital Decade', May 2026; the Flash Eurobarometer 584 also shows that the risks faced online by children are the biggest concerns of Europeans see European Commission, 'Flash Eurobarometer 594: EU Challenges and priorities', June 2026. [Special Eurobarometer on the digital Decade] [Flash Eurobarometer 594]

[23] European Commission, 'Impact of excessive screen time and social media on adolescents' mental health', April 2026. [Flash Eurobarometer FL579]

[24] European Commission: Directorate-General for Education, Youth, Sport and Culture, 'Minutes of the President's Youth Advisory Board', 3 December 2025, accessed 28 July 2026. [PYAB meeting]

[25] Fegert and Melchior, see chapter 3.

[26] 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, ELI: http://data.europa.eu/eli/reg/2022/2065/oj), Article 28(1).

[27] Communication from the 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', (C/2023/6826 final). [Guidelines on the protection of minors].

[28] *Ibid* Article 28(2).

[29] *Ibid* Article 34.

[30] See overview of enforcement actions, European Commission, 'Supervision of the designated very large online platforms and search engines under DSA', updated on 24 July 2026.

preliminary found TikTok and Meta in breach of the DSA for their respective addictive design and in the case of Meta for failing to prevent minors under 13 from using Instagram and Facebook. Preliminary Findings and opened proceedings are an intermediate step in a Commission investigation, and the investigation continues (for opened proceedings) or VLOPs now have the possibility to exercise their right to defence (for preliminary findings), before the Commission decides on next steps in these cases. However, these steps signal the suspicion of potential lack of compliance of these providers.

In addition to the DSA, the Audiovisual Media Services Directive (AVMSD) requires video-sharing platforms (VSPs), irrespective of their size, to take appropriate measures to prevent minors from viewing harmful audiovisual content ([31]), namely to include the EU's media content standards in their terms and conditions, mechanisms to report or flag harmful content, age verification, parental controls and content rating systems. The most harmful type of content, such as pornography or gratuitous violence, must be subject to the strictest measures. It is currently undergoing evaluation and review to identify and remedy potential shortcomings, including whether more should be done to ensure viewers, especially minors, are adequately protected from harm when they view audiovisual content online.

With regard to AI, the Artificial Intelligence Act (AI Act) lays down harmonised rules for the placement on the market, putting into service and use of artificial intelligence ('AI') systems and the placement on the market of general-purpose AI models in the Union aimed at protecting health, safety and fundamental rights, including the rights of children ([32]). First, it prohibits AI systems that deploy subliminal, purposefully manipulative or deceptive techniques and that exploit vulnerabilities due to age. These prohibitions aim to prevent AI systems from manipulating children or exploiting cognitive and other limitations that children may have into taking decisions that they would not have otherwise taken, and to protect them from harmful undue influence, manipulation and exploitation. Second, to help avoid fraud, impersonation and deception, the AI Act obliges providers of AI systems intended to interact directly with natural persons to design and develop those systems in such a way that those persons are informed that they are interacting with an AI system. Furthermore, providers of generative AI systems are obliged to mark and enable detection of AI generated or manipulate content, while deployers of such systems must label deepfakes and published text on matters of public interest produced by such systems without human review or editorial control. Additionally, several AI use-cases with significant impact on minors' rights are classified as high-risk AI systems under the AI Act, such as when used for certain applications in the domain of education and vocational training. High-risk AI systems must meet certain requirements to ensure they are safe and trustworthy, such as risk management, data quality, transparency and human oversight. In particular, the risk management system of a high-risk AI system needs to consider if there is a likelihood of adverse impact on persons under the age of 18 and require appropriate testing and mitigation measures. As regards the most performant general-purpose AI models, their providers must assess and mitigate possible systemic risks at Union level, including risks to the

[31] Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) (OJ L 95, 15.4.2010, ELI: http://data.europa.eu/eli/dir/2010/13/oj)

[32] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

safety and well-being of minors, that may stem from the development, the placing on the market, or the use of the model.

The Commission has also taken steps to combat and prevent child sexual abuse online. In 2022, it presented a proposal for a permanent and comprehensive EU regulatory framework to prevent and combat child sexual abuse, establishing rules for online services providers to prevent the dissemination of child sexual abuse material and the grooming of children. In parallel, the re-cast of the Child Sexual Abuse Directive was recently agreed by the Parliament and the Council extending the scope of criminal offences in view of new risks. The co-legislators also recently enacted new prohibitions under the AI Act for AI systems that generate non-consensual sexually explicit and intimate content or child sexual abuse material; those prohibitions will start to apply on 2 December 2026 ([33]).

The Political Advertising Regulation further introduces specific requirements for the use of targeting and ad delivery techniques in online political advertising that protect children, while allowing minors one year under the voting age to be reached by political advertising ([34]). This enables equal conditions for first-time voters (sometimes as of the age of 16) and allows them to exercise their democratic choices in an informed manner.

In the area of consumer protection law, the Unfair Commercial Practices Directive already protects children as young consumers but the rapidly evolving business models, increasingly sophisticated marketing techniques and the large-scale proliferation of unfair practices underline the urgent need to update the regulatory framework for the digital age and to ensure its effective enforcement ([35]). The Digital Fitness Fairness Check found that consumers, including minors, are in need of enhanced protection online ([36]). The Commission is therefore preparing a proposal for the Digital Fairness Act (DFA) to tackle several problems that consumers face online, including unfair personalisation practices, misleading or obscure pricing practices and problems with managing contracts online, marketing by social media influencers and manipulative commercial practices.

The Better Internet for Kids strategy (BIK+) ([37]) further supports the implementation of this legislative framework, notably the DSA. Under the BIK+, the EU co-funded network of Safer Internet Centres offers training sessions, helplines and hotlines and runs awareness raising

[33] Regulation (EU) 2026/1744 of the European Parliament and of the Council of 8 July 2026 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI) (OJ L, 2026/1744, 24.7.2026, ELI: http://data.europa.eu/eli/reg/2026/1744/oj).

[34] Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising (OJ L, 2024/900, 20.3.2024, ELI: http://data.europa.eu/eli/reg/2024/900/oj).

[35] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2025 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directive Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') (OJ L 149, 11.6.2005, ELI: http://data.europa.eu/eli/dir/2005/29/oj) as amended by Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules (OJ L 328, 18.12.2019, ELI: http://data.europa.eu/eli/dir/2019/2161/oj).

[36] Commission Staff Working Document Fitness check of EU consumer law on digital fairness (SWD(2024) 230 final).

[37] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 'A digital decade for children and youth: the new European strategy for a better internet for kids (BIK+)' (COM/2022/212 final). [BIK+]

activities. They regularly consult children and young people on their needs and view on online safety. In February 2026, the Commission also adopted the Action plan against cyberbullying to prevent cyberbullying, raise awareness and make it easier to report and ensure that victims receive adequate support ([38]).

While legislation already exists to create a safer online environment, no single instrument takes children and their safety and empowerment as the starting point. This initiative addresses this gap and builds upon the existing framework and provide for a dedicated legislative instrument for the protection of minors online, recognising their need for additional protection and providing for clear rules to ensure their protection online.

1.3. Existing and supporting evidence

The proposed Regulation and its accompanying Staff Working Document is underpinned by a solid and robust body of existing evidence. It directly follows on the Report of the Co-Chairs of the Special Panel, which was developed through an independent process that gathered the expertise of more than 60 specialists in diverse relevant fields. It further builds on the extensive evidence and analysis gathered in the context of the Commission's previous and ongoing engagement on the protection of minors online, as well as national and international processes. This rich body of evidence includes a variety of sources as further detailed below.

1.3.1. The Special Panel on child safety online

This independent process brought together more than 60 leading specialists from different fields, including health, child psychology and psychiatry, computer sciences, digital technology and media, social sciences and children's rights. Representatives from youth groups, parents' groups and children's rights organisations also participated. The Special panel on child safety online examined risks and opportunities for children on digital services as well as the regulatory framework and gathered extensive data. Additional stakeholders provided input throughout the process such as the OHCHR, specialised think-tanks, industry representatives, regulators from third countries as well as the European Data Protection Board. The Co-Chairs of the Special Panel also had additional meetings with representatives of Member States as well as the European Parliament and its Members, especially of the Intergroup on Children's Rights. Informed by the meetings of the Special Panel, the Co-Chairs presented their Report in July 2026 to the President of the Commission ([39]). The Report is intended to inform future actions and provides for an analytical assessment on how to better protect and empower minors online.

1.3.2. Existing Impact Assessments

As previously noted, the proposed Regulation does not exist in a regulatory vacuum but is a part of a broader legislative framework underpinned by existing impact assessments, and consultation processes. This Staff Working Document builds on data and analysis conducted in relation to the upcoming legislative proposal of the DFA, the evaluation and review of the AVMSD, the Regulation to combat and prevent child sexual abuse and the re-cast of the Child

[38] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Action Plan against cyberbullying "Safer online, stronger together"' (COM/2026/71 final). [Action Plan against cyberbullying]
[39] Fegert and Melchior.

Sexual Abuse Directive and their accompanying Impact Assessment ([40],[41]), the DSA and the Digital Market Act (DMA) and their accompanying Impact Assessments ([42],[43]) as well as the AI Act and its accompanying Impact Assessment ([44]).

In relation to the DFA, the consultation and call for evidence was opened for 12 weeks on 17 July 2025, collecting extensive feedback from citizens, public authorities and other stakeholders, which compiled relevant evidence on addictive design of digital products and deceptive or manipulative interface design, including the impact on such practices on minors. The exercise built on the Commission's 2024 Digital Fairness Fitness Check, and sought input on practices such as dark patterns, unfair influencer marketing, addictive design, unfair personalisation, unfair pricing and issues with digital contracts and simplification rules. The Commission published its summary report of the consultation on 19 December 2025 ([45]). Furthermore, on 10 February 2026 the Commission launched a public consultation for the assessment of the Impact of the AVMSD, collecting feedback from an equally wide range of stakeholders, including on the best ways to strengthen the protections for minors online. Both consultative processes provided relevant evidence for the purpose of this proposal.

1.3.3. DSA Implementation and enforcement

In addition to the work preceding the adoption of the DSA, significant evidence and data have been collected during the two years of its implementation and enforcement. In terms of enforcement, and as previously mentioned, the Commission adopted 10 preliminary findings in relation to the protection of minors, and several enforcement cases are still ongoing ([46]). For instance, the Commission adopted preliminary findings against TikTok for failing to ensure safe accounts for minors ([47]) and for its addictive design, including features such as infinite scroll, autoplay, push notification and its highly personalised recommender system ([48]), as well as

[40] Commission Staff Working Document, Impact Assessment Report accompanying the document Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse (SWD (2022) 209 final). [Impact Assessment CSAR]

[41] Commission Staff Working Document Impact Assessment Accompanying the document Proposal for a Directive of the European Parliament and the Council on combating child sexual abuse material, and replacing Council Framework Decision 2004/68/JHA (recast). [Impact Assessment CSAD]

[42] Commission Staff Working Document Impact Assessment Accompanying the Document Proposal For a Regulation of the European Parliament and of The Council on a Single Market For Digital Services (Digital Services Act) and Amending Directive 2000/31/EC, 2020 (SWD(2020) 363 final). [DSA Impact Assessment]

[43] Commission Staff Working Document Impact Assessment Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), 2020 (SWD(2020) 364 final). [DMA Impact Assessment]

[44] Commission Staff Working Document Impact Assessment Accompanying the Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (SWD(2021) 84 final). [AI Act Impact Assessment]

[45] European Commission, *Have you say – Digital Fairness Act Public Consultation*.

[46] See overview of enforcement actions, European Commission, 'Supervision of the designated very large online platforms and search engines under DSA', updated on 24 July 2026.

[47] European Commission, Commission preliminary finds TikTok in breach of Digital Services Act for failing to ensure safe accounts for minors | Shaping Europe's digital future, July 2026

[48] European Commission, Commission preliminarily finds TikTok's addictive design in breach of the Digital Services Act | Shaping Europe's digital future, February 2026

preliminary findings against Meta for failing to prevent minors under 13 from using Instagram and Facebook ([49]) and related to addictive design of those platforms ([50]).

The protection of minors is also a main focus for several other sources of information that are available to the Commission in the context of the implementation and enforcement of the DSA, in particular the annual transparency reports, Risk Assessment reports, audit reports required to the VLOPs and VLOSEs ([51]), and the Commission Reports on the risk assessment cycles ([52]), as well as dedicated stakeholder engagement action carried out by the Commission, in particular dedicated workshops with a focus on Risk Assessment ([53]) and several roundtables with civil society ([54]). Relevant studies on the protection of minors are also conducted on an ongoing basis under the DSA.

1.3.3.1. Development and adoption of the Guidelines on the protection of minors

Additionally, the guidelines on the protection of minors were developed following a comprehensive process which included a call for evidence ([55]), stakeholder workshops held in October 2024 ([56]) and June 2025 ([57]), a targeted public consultation ([58]), further engagement with children and young people ([59]) and meetings of the European Board for Digital Services within its working group on the protection of minors ([60]). The 2024 call for evidence received more than 170 replies ([61]), and the 2025 public consultation more than 300 inputs providing detailed information from a wide range of stakeholders including researchers, civil society, industry, public authorities on good practices and measures for online platforms to design their services in line with Article 28 DSA ([62]).

---

[49] European Commission, *Commission preliminarily finds Meta in breach of Digital Services Act for failing to prevent minors under 13 from using Instagram and Facebook* , April 2026

[50] European Commission, *Commission preliminarily finds the addictive design of Instagram and Facebook in breach of the Digital Services Act | Shaping Europe's digital future*, July 2026

[51] All transparency reports, transparency database, and public versions of the risk assessment reports are published at: European Commission, *How the Digital Services Act enhances transparency online*, 2026.

[52] European Commission, *Digital Services Act report lays out landscape of systemic risks online | Shaping Europe's digital future* , November 2025.

[53] European Commission, *The Commission holds workshop with platforms and civil society on the assessment of online risks | Shaping Europe's digital future,* June 2025.

[54] European Commission, *Fourth roundtable with Civil Society Organisations on the implementation of the Digital Services Act | Shaping Europe's digital future*, February 2026.

[55] European Commission, *Commission launches call for evidence for guidelines on protection of minors online under the Digital Services Act | Shaping Europe's digital future*, July 2024

[56] European Commission, *Commission gathers good practices to combat online harm for minors | Shaping Europe's digital future,* October2024

[57] European Commission, *European Commission hosts expert consultation workshop on draft guidelines on protection of minors under the DSA | Shaping Europe's digital future*, June 2025

[58] European Commission, *Commission seeks feedback on the guidelines on protection of minors online under the Digital Services Act | Shaping Europe's digital future*, May 2025

[59] European Commission, *Digital Services Act: Commission publishes report on European and national focus groups with young people on the protection of minors guidelines | Shaping Europe's digital future*, July 2025

[60] European Commission, *Working Group 6 of the European Board for Digital Services – Protection of Minors | Shaping Europe's digital future*, 2024

[61] European Commission, *Digital Services Act: Summary report of the call for evidence for the protection of minors guidelines | Shaping Europe's digital future*, July 2025

[62] European Commission, *Digital Services Act: Summary report of the targeted public consultation on protection of minors guidelines | Shaping Europe's digital future*, July 2025

1.3.4. Continuous engagement with national authorities and stakeholders

Additional evidence sources are received on a continuous basis from the European Board for Digital Services ("the Board") and the national Digital Services Coordinators. Protection of minors, recognised as "a core value and objective of the Board", has continuously been a priority in the activities of the Board ([63]). During all its meetings of the Board, Digital Services Coordinators had the opportunity to update the Board of national developments related to child safety online at national level. The Board also harbours a dedicated working group on the protection of minors ([64]) where issues related to the protection of minors, in particular Article 28 DSA and the Guidelines, focusing on priority topics such as age assurance, recommender systems, online interface design and risk reviews. It also provides support to national authorities as regards the roll out of the EU Age Verification blueprint.

Furthermore, national authorities have supported the Commission's enforcement work and provided valuable inputs for the preliminary findings on 4 pornographic platforms allowing minors to access their services ([65]). The opening of investigations into Snapchat compliance with the DSA - on the protection of minors - in March 2025 also relied on substantive evidence transmitted by Digital Services Coordinators (such as the German and Dutch Digital Services Coordinators). As part of a memorandum of understanding, ACM has seconded an official to closely cooperate with Commission's services as part of the investigations.

Engagement with national authorities and stakeholders active in the protection of minors at national level has also been supported by the deployment of DSA Officers in the representation of the European Commission in all 27 Member States. As Commission's staff stationed in the Member States, they have engaged since March 2025, with national stakeholders such as designated trusted flaggers ([66]) or national Safer for Internet Centres ([67]) to collect evidence and information of the challenges related to the protection of minors. Finally, they have informed the Commission services of national initiative's aiming at having a better understanding of the impact of certain platforms on the mental health and well-being of youth.

Member States conducted national inquiries and consultative processes with regards to the protection of minors online. In June 2026, the German Commission of Independent Experts on the Protection of Children and Young People in the Digital World presented its 56 recommendations for action for better child and youth protection in the digital world ([68]). The Swedish Inquiry also published its interim report analysing the conditions for the introducing an age limit for minors' use of social media in Sweden, in particular in light of fundamental rights and freedoms ([69]). In 2024, the report 'Enfants et écrans' was delivered to the French President, Emmanuel Macron, highlighting the role of screens on health and children's development and proposing several recommendations to ensure an age-appropriate use of

[63] European Board for Digital Services, *Annual Work Programme, Q4/2025 to Q4/2026*, November 2025.
[64] European Board for Digital Services, *Working Group 6 of the* European Board for Digital Services – Protection of Minors, November 2025.
[65] European Commission, *Commission preliminarily finds PornHub, Stripchat, XNXX and XVideos in breach of the Digital Services Act for allowing minors to access their services*, May 2026.
[66] European Commission, *Trusted flaggers under the Digital Services Act (DSA)*.
[67] European Commission, *Safer Internet Centres*.
[68] Handlungsempfehlungen der Unabhängigen Expertenkommission "Kinder- und Jugendschutz in der digitalen Welt" , *'Entwicklung stärken, Verantwortung übernehmen: Für ein gutes Aufwachsen von Kindern und Jugendlichen in der digitalen Welt'*, June 2026.
[69] Krafft, L. et al., *Interim Report: An age limit for children's access to social media*, SOU 2026:35, State Public Investigations, June 2026. [SE Interim Report]

screens ([70]), followed by the Inquiry Commission on the Psychological Effects of TikTok on Minor ([71]) of the French National Assembly. In the context of their ongoing national processes, Austria and Norway also conducted impact assessments regarding their proposals for a minimum age ([72],[73]).

1.3.0. International engagement

DG CNECT concluded a series of cooperation arrangements with front runner regulators, including with the UK's Ofcom ([74]), Australia's eSafety Commissioner ([75]) Brazil's National Data Protection Authority ([76]), and Japan's Ministry of Internal affairs and Communication ([77]). DG CNECT is in regular contact via Digital Partnerships and Dialogues with other jurisdictions such as Singapore, Canada, and Switzerland ([78]). On 7 November 2025, DG CNECT, Ofcom and the eSafety Commissioner, launched a trilateral technical cooperation group on age assurance to further explore ongoing regulatory and policy developments, including the Australian Social Media age restrictions' implementation ([79]).

These arrangements facilitate the cooperation and sharing of experience at global level. Key insights include the Australian impact assessment underpinning the Online Safety Amendment (Social Media Minimum Age) Act 2024, the eSafety Commissioner's March 2026 compliance report and the second report co-developed by the eSafety Commissioner in partnership with Stanford University ([80],[81]). The evidence and enforcement of the Brazilian ECA Digital by the Brazilian Data Protection Authority (ANPD), covering strong provisions to ensure a high level of safety and privacy for minors including the prohibition of lootboxes, parental control tools and implementation of age assurance ([82]), also contributed to the available evidence-base. Additionally, the United Kingdom, and more specifically OFCOM as the relevant independent regulator, has gathered significant evidence in the context of the adoption of the Online Safety Act and its implementation. This evidence includes an impact assessment, as well as several reports procured by OFCOM.

At multilateral level, protection of minors online has become a priority area for action with a growing body of evidence and expertise emerging across jurisdictions. On 17 June, the G7 Leaders launched a call on different jurisdictions to support a safer and more secure digital space for minors including with measures against addictive features, safety by design and age

[70] Bousquet-Bérard, C., Pascal, A., *Enfants et écrans : à la recherche du temps perdu*, 2024.
[71] Assemblée Nationale, Commission d'enquête sur les effets psychologiques de TikTok sur les mineurs, 2025
[72] Impact Assessment accompanying the Federal Act amending the Audiovisual Media Services Act and the KommAustria Act (2026/0405/AT). [AT Impact Assessment]
[73] Supplementary information about the draft Act and Impact Assessment (2026/90007/NO).
[74] European Commission, *Commission services sign administrative arrangement with Ofcom to support the enforcement of social media regulations,* 16 May 2024.
[75] European Commission, *Commission services sign administrative arrangement with Australian eSafety Commissioner to support the enforcement of social media regulations*, 11 June 2024.
[76] European Commission, *Commission services cooperate with Brazil's Data Protection Agency on protection of minors online*, 12 June 2026.
[77] European Commission, *Commission services sign cooperation arrangement with Japan's Ministry of Internal Affairs and Communications to support the enforcement of digital platform regulation*, 5 May 2026.
[78] European Commission, *Digital partnerships | Shaping Europe's digital future*, 12 May 2026.
[79] European Commission, *The Commission, Australia's eSafety Commissioner, and UK's Ofcom share insights on age assurance measures*, February 2026.
[80] eSafety Commissioner, *Social Media Minimum Age: Compliance Update*, 2026. [eSafety Compliance Update 2026]
[81] eSafety Commissioner, *Early Days Early Insights - Social Media Minimum Age Restrictions Report*, 2026. [eSafety Early Insights 2026]
[82] BR ECA Digital.

assurance ([83], [84]). This G7 leaders' call builds on G7 principles on the protection of minors online, which acknowledge that the use of digital services 'can lead to compulsive, habit-forming, and other problematic uses and behaviours, which may impact self-esteem and further threaten their [minors'] health' ([85]).

1.3.1. Youth Consultations

In its meeting of December 2025, the President Youth Advisory Group discussed age restrictions and online safety in the digital environment ([86]). The Youth Advisory Group brings together more than 30 young representatives, one from each EU Member State's National Youth Council, one from the European Youth Forum, and observers from candidate countries and potential candidates for EU accession. During their meeting, the Group discussed the benefits and risks of social media, the importance of digital literacy as well as the need to ensure that digital service providers are held accountable for their services.

The EU co-funded network of Safer Internet Centres also plays a central role in supporting child participation at national level as well as in analysing and understanding online safety risks through their helplines and hotlines. Together with the Better Internet for Kids (BIK+) platform, the network reached 46 million people in 2025 alone, a presence and reach that is regularly translated into feedback to national authorities and the Commission on emerging trends and priorities in the field of child online safety. In particular, the network also supports BIK+ Ambassadors that represent children and youth in several instances on child online safety, such as the Safer Internet Forum, the national events on Safer Internet Day or the European Forum on the Rights of the Child. In December 2025, the annual Safer Internet Forum, which involved over 200 children, young people and representatives from civil society, industry and national authorities, discussed the topic of age restrictions to social media, approaches to online safety and respecting children's rights ([87]).

In the context of the preparation and adoption of the action plan against cyberbullying, a wide variety of stakeholders have been consulted, including children and young people through targeted and public consultations. Thanks to the Commission's survey carried out via the EU Children's Participation Platform, 6300 children were able to give their inputs on cyberbullying and help shape the action plan ([88]). The EU Children's Participation Platform was also used in the context of a consultation linked to the upcoming Digital Fairness Act. Questions were also raised in relation to rules for joining social media. In total, 4,786 children aged 12-17 were from all EU Member States and EU citizens living abroad took part in the survey. Children emphasised that they want the online environment to be safer, with stronger rules for services ([89]).

---

[83] European Commission, *Commission welcomes G7 agreement on common principles for protecting minors online | Shaping Europe's digital future*, 29 May 2026

[84]Elysee, *Leaders' call on a safer digital space for minors. | G7 Évian 2026*, 17 June 2026.

[85] G7 Call Safer Digital Space for Minors.

[86] PYAB meeting.

[87] European Commission, *Safer Internet Forum (SIF) 2025*, 2025

[88] European Commission, *EU Children's Participation Platform – Cyberbullying, reporting results from the 2025 consultation of 6,300 children aged 12–17*, 2025. [Cyberbullying report]

[89] European Commission, *EU Children's Participation Platform – Findings form the consultation with children on The Digital Fairness Act (DFA)*, 2026.

1.3.2. Additional studies

Between March and April 2026, the Commission conducted a Eurobarometer survey on the impact of excessive screen time and social media on young people's mental health collecting data from more than 26,000 13-18 years old and more than 12,000 parents across all 27 Member States ([90]). The annual survey carried out in the context of the State of the Digital Report as well as the Special Eurobarometer on the digital Decade provided additional data points in terms of the growing and sustained concern for Europeans to protect children online ([91],[92]).

In August 2026, the Commission procured an additional study ('the external study') for the purpose of complementing the existing body of evidence and support the proposed Regulation and its accompanying Staff Working Document. The study examines the impact of age assurance on the fundamental rights of children as well as adults and analyses the economic impacts of implementing age assurance solutions from the perspective of the services and systems in scope. The results of the study are expected to be finalised and published in Q4 2026.

Taken together, this body of evidence and consultation processes constitute a solid foundation for the proposed Regulation and underpin the findings of its accompanying Staff Working Document.

2. STATE OF PLAY AND PROBLEM STATEMENT: THE PROTECTION OF MINORS IN THE EUROPEAN UNION

The proposal for a dedicated instrument for the protection of minors online responds to several identified problems regarding the safety of minors in the online environment. These problems include (1) a fragmented internal market, (2) an evolving online environment with certain services and systems that are risky and not appropriate for minors and (3) a lack of clear requirements for age assurance.

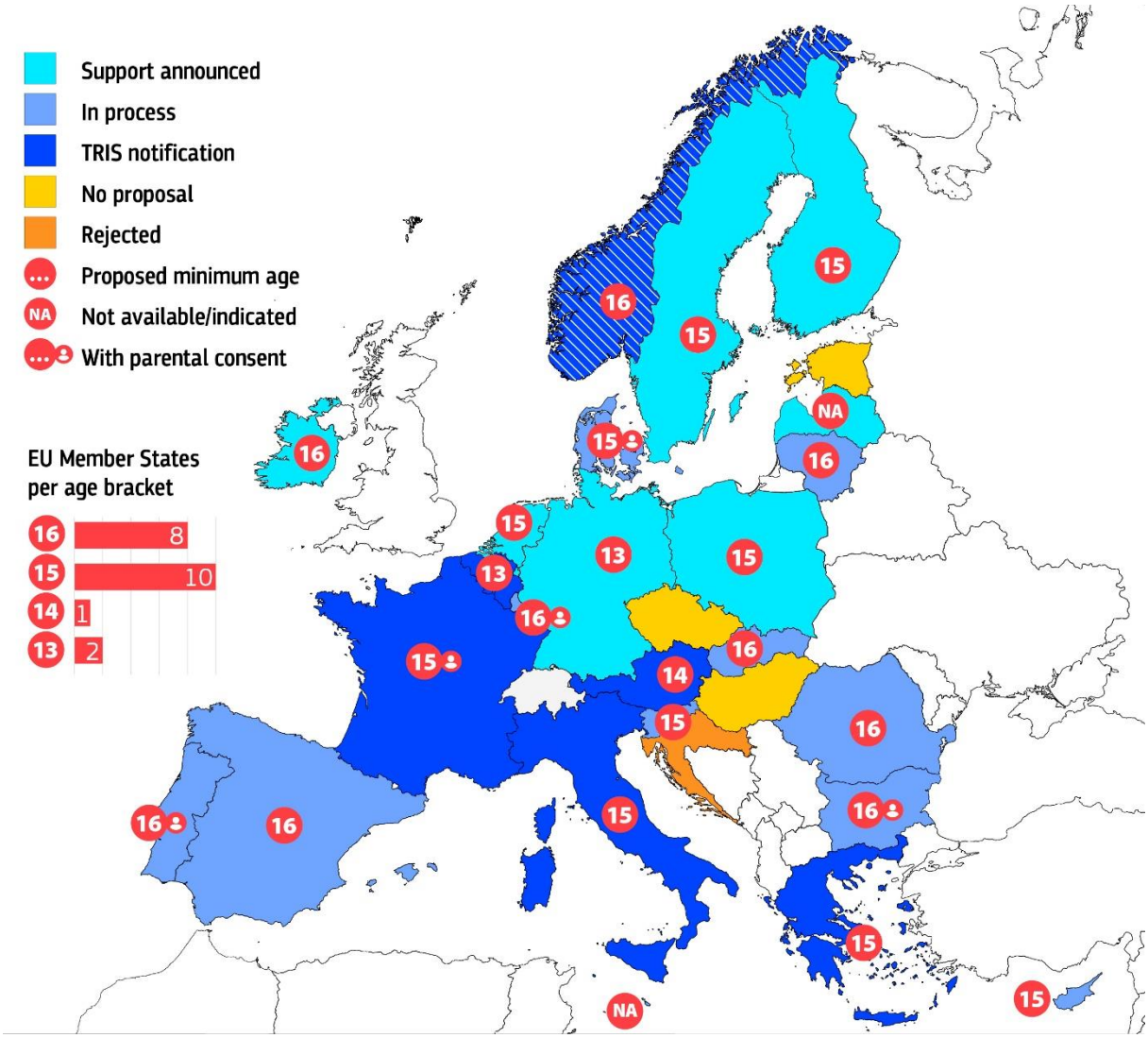
2.1. A fragmented internal market

Across the European Union, Member States are discussing or adopting new measures restricting access to certain online services considered risky for children under a specified age ([93]). In July 2026, the French Parliament voted on a national measure restricting access to social media for under 15 years old which was foreseen to enter into force in September 2026 and is pending a review following a negative decision of the Constitutional Court ([94]). Several other Member States are well advanced in their process of adopting similar measures. The draft national laws were notified by France in April 2026 ([95]) and in September 2026 ([96]), Italy ([97]), Greece ([98]),

[90] Flash Eurobarometer FL579.
[91] Special Eurobarometer on the Digital Decade and
[92] Flash Eurobarometer 594.
[93] Fegert and Melchior, pp.104-105.
[94] Assemblée nationale, 'Proposition de loi visant à protéger les mineurs des risques auxquels les expose l'utilisation des réseaux sociaux', 20 July 2026. [Assemblée nationale]
[95] Legislative provisions aimed at protecting minors from the risks to which they are exposed by the use of social networks (2026/0185/FR). [Notification 2026/0185/FR]
[96] Projet de loi visant à protéger les mineurs des risques auxquels les expose l'utilisation des réseaux sociaux (2026/0500/FR).
[97] Draft law on the protection of minors in the digital dimension (2025/0235/IT).
[98] Notification to the European Commission of draft provisions on the introduction of a minimum age limit for the use of online social networking services, in accordance with the procedures of Presidential Decree 81/2018 (2026/0233/GR). [Notification 2026/0233/GR]

Austria ([99]), Norway ([100]) and Belgium ([101])to the Commission in the course of 2025 and 2026. Entry into force is expected for Greece and Austria in January 2027.

Consultative processes have also been set up in several Member States. In June 2026, Germany's expert committee and Sweden's inquiry concluded with recommendations respectively proposing a minimum age limit at 13 ([102]) and of 15 ([103]). In almost all other Member States, legislation has been announced by governments or is being discussed in national parliaments. Several Member States have also indicated a preference for action at European level. Figure 1 provides an overview of national developments; it includes the stage of the process, the ages being proposed, and whether parental consent is being considered ([104]).



[99] Federal Act amending the Audiovisual Media Services Act and the KommAustria Act (2026/0405/AT).
[100] Draft act introducing an age limit for social media use (2026/9007/NO). [Draft act 2026/9007/NO]
[101] Draft decree amending the decree of 27 March 2009 on radio broadcasting and television in relation to the protection of minors in brokering services that may affect their physical, mental or moral development (2026/0458/BE). [Draft decree 2026/0458/BE]
[102] Commission of Independent Experts on the Protection of Children and Young People in the Digital World, 'Strengthening development, taking responsibility: Recommendations for action', June 2026.
[103] SE Interim Report.
[104] This table is only a reflection of the state of play as of 7 September 2026.

Figure 1: Overview of national developments as of 7 September 2026.

The legislations discussed at national level differ in several aspects including their scope, age limits and types of restrictions.

2.1.1. Differences in proposed scope

In terms of scope, some Member States, such as Greece ([105]) and France ([106]), define the restricted services as online platforms under the DSA that can be considered as an online social networking service as defined under the Digital Markets Act (DMA). Norway is additionally considering the further criterion of "harmful" defined as "a service that, through its design, features or content, can be harmful to children's emotional, cognitive or health development or safety" to limit the scope of the access restrictions ([107]). Austria, on the other hand, defines the scope of their restriction based on the definition of a VSP under the AVMSD which offers at least one functionality considered harmful to minors ([108]). The law sets out a non-exhaustive list of such functionalities, the supervisory authority being empowered to identify others as appropriate. The draft notified by Italy proposes to restrict access to both social media services and VSPs. Belgium takes another approach combining a broad scope 'intermediary services' with a qualitative criterion of 'negatively impact the physical, mental or moral development of minors' similar to Norway. This criterion would be assessed by the Flemish Government which would then prepare a list of the services to fall within the scope of the age restriction ([109]).

2.1.2. Differences in proposed age limits

In terms of age, the Greek and French draft legislation prohibits access to under-15s. In Norway, under the current draft, the age limit would be set at 16. Some Member States have also proposed different ages including 13 and 14 ([110]). Additionally, allowing for a lower age limit with parental consent is discussed in for example Denmark and Greece ([111]). It should be added that while some legislation relies on the actual age of the minor, some refer to the year in which the minor turns a certain age ([112]).

[105] Notification 2026/0233/GR.
[106] Assemblée nationale.
[107] Draft act 2026/9007/NO.
[108] Supplementary information about the draft Act and impact assessment (2026/9007/NO), p.8.
[109] Draft decree 2026/0458/BE.
[110] Fegert and Melchior, pp.104-105.
[111] For instance, the Greek notified draft refers to 1 January as the date of the birth for all persons born within the same year.
[112] Notification 2026/0233/GR.

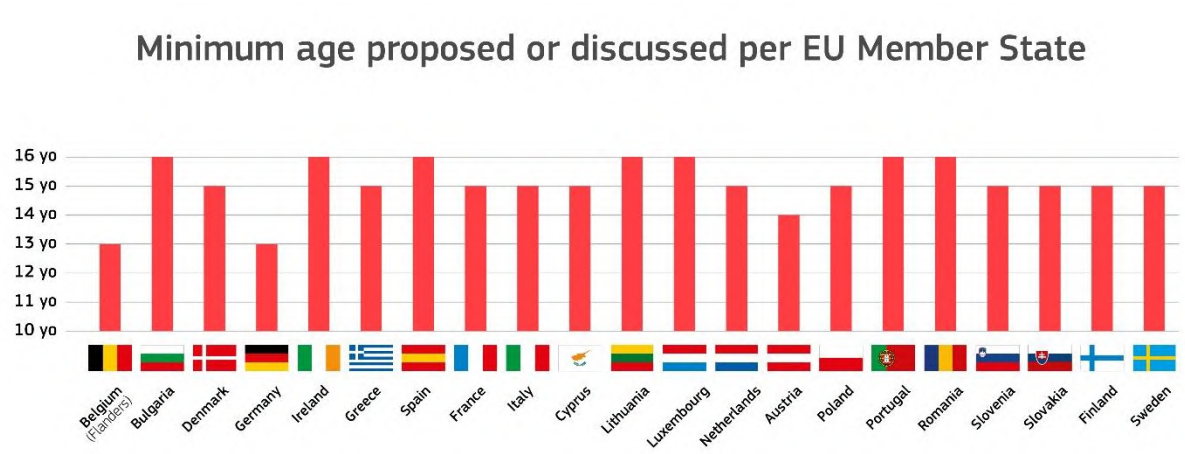


Figure 2 Minimum age proposed or discussed by EU Member State as of August 2026

2.1.3. Differences in the proposed restrictions and additional measures

In terms of types of restrictions, national drafts refer to limiting "access". It remains unclear whether this would focus on account creation, as suggested by the French first notified draft ([113]), or if this would extend to overall access to a service. Account restrictions are different from an access restriction: an account restriction might not limit access to certain parts or content of the service which may be accessible without a log-in.

Some Member States are proposing and discussing legislation going beyond establishing a minimum age by also providing additional requirements regarding age assurance or obligations relating to safety-by design. Greece, for instance, requires that providers in scope apply appropriate, proportionate and reliable age verification methods, which can be supplemented by age estimation methods when deemed necessary ([114]). Austria's notified draft also outlines requirements for age verification including data minimisation, functional separation between the VSP and the age verification provider, non-traceability of the age credentials and interoperability amongst others ([115]).

2.1.4. Legal uncertainty, compliance costs and an unequal level of protection for minors

In practice, the emergence of diverging national laws is already leading to a fragmented internal market. Access to a specific online service might be delayed in one Member State but not in others, depending on the scope of the legislation and its exemptions. Additionally, it might be restricted for different age groups and subjected to parental consent in only some Member States. The practical implementation of these national laws might also differ in terms of entry into force, application to access or accounts, specific requirements for age verification and enforcement frameworks.

Those diverging national measures impact the provision of digital services and possibly could extend in the future to other systems (such as certain chatbots), a market that is inherently cross-border in nature and operates across the European Union. It leads to significant compliance burdens for providers of such services and systems, including for certain small and micro

[113] Notification 2026/0185/FR.
[114] Notification 2026/0233/GR.
[115] Draft act 2026/0405/AT

enterprises which are included in the scope of some national measures. As large competitive advantages already exist, it creates an additional barrier for scaling-up and increases the competitive advantage for companies large enough to absorb such costs.

Furthermore, this patchwork of national measures gives rise to enforcement difficulties. Under the current legal framework, authorities from Member States may have to enforce the access restrictions of other Member States against providers established in their territory. This would require competent authorities to have knowledge and understanding of the measures taken by all other Member States, as well as multiply processes and procedures for enforcing restrictions.

Children will also face different levels of protection across the European Union, where they will be able to access different services at different ages, with a three-year gap between certain Member States, and under different circumstances. This sends contradictory messages to parents and children alike about the age-appropriateness of certain services and the risks associated with them. The lives of children may not be constrained to one Member State, as children might have families or friends living in a different Member State, or simply go to school or spend long periods of time in a different Member State than that in which they reside. This impacts the effective implementation of those measures, and the normative change sought. Peer pressure and social expectations will remain for children to join the online services concerned at a young age.

Overall, emerging national legislation will create a patchwork of access restrictions leading to a complex and uncertain regulatory environment for digital services and possibly other systems that could be affected in the future, creating an uneven level of protection for minors across the European Union, enforcement complexity and compliance costs.

2.2. An insufficient level of protection for minors online

Children's lives are increasingly shaped by the online environment, which is now deeply embedded in their social, educational and leisure activities, as well as their development. However, this growing digital engagement is not matched by an equivalent sense and standard of safety. Across Europe, **only 48% of children aged 9–16 report feeling safe online**, while many also recognise that they **spend too much time on the internet** ([116]). Children are going online at younger ages and spending more time online as they grow older ([117],[118]). By adolescence, screen use occupies a substantial part of daily life. In Europe, young people aged 13-18 report spending an average of 4.5 hours a day on screens on school days and 6.1 hours a day at weekends; nearly half (46%) spend more than 6 hours a day, and 14% spend more than 10 hours ([119]).

2.2.1. The risks faced by children online

During the time spent online, children are exposed to many risks. As detailed in the Report of the Co-Chairs of the Special Panel, **these risks are wide-ranging and often interconnected.** They include exposure to harmful or age-inappropriate content, cyberbullying, unwanted

[116] Staksrud, E., Livingstone, S., Ólafsson, K., 'Use, Views and Worries on Age Bans on Social Media: Responses from 29,169 children in 19 European countries', *EU Kids Online 2026*, Report No 2, 2026. [EU Kids Online 2026]
[117] Children under 2 use screens for an average of 49 minutes per day, rising to around 3 hours per day by age 8. Source: Rideout, V., *The Common Sense Census: Media Use by Kids Age Zero to Eight*, 2020.
[118] Taylor, G., Sala, G., Kolak, J., Gerhardstein, P., Lingwood, J. , 'Does adult-child co-use during digital media use improve children's learning aged 0–6 years? A systematic review with meta-analysis', *Educational Research Review*, 44, 100614, 2024.
[119] Flash Eurobarometer FL579.

contact from strangers, infringements of privacy and dignity, and serious adverse effects on mental and physical health. The Report also stresses that these risks often overlap and may affect some groups of minors more severely, including children with disabilities, those from minority backgrounds, and those with pre-existing mental health difficulties ([120],[121],[122],[123],[124],[125],[126],[127],[128],[129]).

Table 1 below synthesises a range of risks categories that children frequently encounter online, drawing on the Report of the Co-Chairs of the Special Panel alongside additional evidence from EU institutions, regulators and independent research.

Table 1 Overview of risks minors face online.

Risk Category	Key Evidence
Cyberbullying	In the 2025 EU consultation, 24% of children aged 12-17 reported having experienced cyberbullying, 39% said they had witnessed it, and 50% knew someone who had been targeted ([130]). Despite how widespread the problem is, many young people feel services are not doing enough. Around 75% of adolescents rate current platform measures as ineffective, or only fair to poor ([131]).
Harmful or age-inappropriate content	Children are frequently exposed to material depicting or encouraging self-harm, eating disorders ([132]), suicide and other severe harms, and such exposure is likely to aggravate pre-existing vulnerabilities. The Children's Online Experiences Research Report (2026) found that 73% of 11-17 years-olds had been exposed to at least one type of harmful content over a four-week period, while 31% had encountered the most severe kind,

[120] Ronis, S., Slaunwhite, A., 'Gender and Geographic Predictors of Cyberbullying Victimization, Perpetration, and Coping Modalities Among Youth', *Canadian Journal of Psychology*, 34 (1), 2017.
[121] Koch, T., Laaber, F., Florack, A., 'Socioeconomic status and young people's digital maturity: The role of parental mediation', *Computers in Human Behaviour*, 154, 2024.
[122] Li, H., Luo, M., Duan, B., Kawulia, A., Su, M., Di, H., 'Family socioeconomic status and young children digital addiction: a moderated mediation model', *Frontiers in Psychology*, 27 (5), 2024.
[123] Lu, Z., 'Mapping adolescent problematic social media use patterns across 41 countries/regions: A multilevel latent class analysis with social determinants', Addictive Behaviors, 172, 2026. [Lu]
[124] Gracia, P., et al., World Happiness Report 2026, 2026, Chapter 7: Problematic social media use and adolescent wellbeing: the role of family socioeconomic status across 43 countries. Wellbeing Research Centre, University of Oxford. [World Happiness Report]
[125] Prkno, D., Grafe, N., Schulz, M.S., Kiess, W., Poulain, T.,'Children's and adolescents' negative internet experiences and the association with quality of life and behavioural difficulties: a cross-sectional study', *BMJ Paediatrics Open*, 17:9 (1), 2025. [Prkno]
[126] Ofcom, *Research into risk factors that may lead children to harm online*, 2022, p. 27.
[127] eSafety Commissioner, *A new playground: The digital lives of young people with disability*, 2023. [eSafety Commissioner 2023].
[128]Childlight Global Safety Institute, *The nature of online CSEA among children living with disabilities*, 2023.
[129] Villar Onrubia, D., Barreda Angeles, M., Cachia, R., Economou, A., Lopez Cobo, M., *Cyberbullying: Insights from science, policy and legislation*, Publications Office of the European Union, Luxembourg, 2025, JRC144335.
[130] Cyberbullying report.
[131] Vogels, E, *Teens and Cyberbullying 2022*, Pew Research Center: Internet, Science and Tech, United States of America, 2022.
[132] E.g. the "Pro-Ana" movement, a network of online communities that promotes and normalises disordered eating behaviour, reorganising around shifting hashtag to evade platform moderation. Source: Sala, A., Porcaro, L., and Gómez, E., 'Social Media Use and adolescents' mental health and well-being: An umbrella review', *Computers in Human Behaviour Reports*, vol. 14, 2024, p. 8. [Sala et al.]

	including pornography, suicide, self-harm and eating disorder material ([133]).
Privacy and dignity infringements	Inadequate safeguards around the collection and retention of children's personal data can expose minors to serious privacy harms. One example illustrating this risk in the U.S. Department of Justice's settlement with unlawfully collected and retained personal data from children under 13 without parental consent and failed to delete their accounts even after made aware of their age ([134],[135]).
Unwanted contact from strangers	According to a 2023 study by Common Sense Media, nearly six in ten adolescent girls reported having been contacted by a stranger on social media platforms in a way that made them feel uncomfortable ([136]). Ofcom reports that among children who game online, over half (55%) said they play with people they have not met in real life at least sometimes, and one in five (20%) do so frequently ([137]). This finding is consistent with large-scale expert consensus identifying several platform design features, including anonymous profiles, direct messaging functionalities, and broad user reach, as mechanisms that may facilitate predator access to children and support grooming behaviour ([138]).
Problematic or excessive use	These risks are reflected in both behavioural patterns and reported health symptoms. An EPRS study across six European countries found that 97% of young people use the internet daily and that 78% of those aged 13-17 check their device at least once an hour, with more than a quarter displaying behaviour resembling addiction ([139]).
Disinformation and misinformation	About half of children encounter misinformation weekly by age 8 ([140]), rising with age; up to 70% of young people in the EU report lacking the skills to recognise disinformation online ([141]).
Body image concerns and	Content promoting eating disorders and "thin-ideal" imagery ([142]), often evading moderation through evolving hashtags, is linked to body image

[133] Within this category, eating disorder content was the most recalled (23%), followed by pornography (11%) and suicide or self-harm content, seen by 14% if children overall. Source: Ofcom, *Children's Online Experiences*, 2026. [Ofcom Children's Online experiences research report]

[134] Federal Trade Commission. (n.d.). United States v. ByteDance Ltd. FTC Legal Library, Cases and Proceedings. Retrieved August 26, 2026, from https://www.ftc.gov/legal-library/browse/cases-proceedings/bytedance-ltd-us-v

[135] S. Department of Justice, Office of Public Affairs, *Justice Department secures $400M settlement with TikTok and ByteDance to resolve children's privacy litigation*, August 202.

[136] Common Sense Media, *How Girls Really Feel About Social Media*, 2023.

[137] Ofcom Children's Online experiences research report.

[138] Capraro, V., et al., A collective review on some potential negative impacts of smartphone and social media use on adolescent mental health: Results from a Delphi process', *Seton Hall Law School Legal Studies Research Forthcoming HEC Paris Research Paper No. MKG-2025-1567,* 2025.

[139] European Parliamentary Research Service (EPRS), Scientific Foresight Unit (STOA), *Harmful internet use – Part I: Internet addiction and problematic use*, PE 624.249, European Parliament, 2019.

[140] Adler Berg, F., et al., 'Children and misinformation on social media: A Scoping review', *Global Studies of Childhood*, 2025.

[141] Howard, P.N., et al., *Digital Misinformation / disinformation and children*', UNICEF, 2021.

[142] Sala et al.

eating behaviours	dissatisfaction and eating disturbances, particularly among girls form as young as age 10 ([143]).
Alcohol and substance abuse	Exposure to and sharing of alcohol-related content is associated with higher drinking in a bidirectional reinforcement loop; substance-related content is linked to higher rates ([144], [145]).
Child sexual abuse material and grooming	63% of all children sexual abuse webpages found by the Internet Watch Foundation in 2025 were hosted in EU Member States ([146]). More than half of respondents of a global study from 2021 had experienced a form of child sexual abuse online ([147]). According to 2025 data from the United States' National Centre for Mission and Exploited Children (NCMEC), online grooming is expanding at an alarming rate, with reports increasing by 158% over the past three years ([148]).
Radicalisation and recruitment for terrorism	Social media, encrypted messaging and online communities are used to disseminate propaganda and recruit minors, including through gaming environments; nearly one third of individuals arrested in the EU in 2024 for terrorism-related offences were minors or young adults ([149]), with recruitment documented among children as young as 8 or 9.

These risks, individually and in combination, carry serious consequence for children's mental health and well-being. Adolescents are already a particularly vulnerable group when it comes to mental health. In Europe 59% of young people report [150]emotional or psychosocial difficulties ([151]). A growing body of evidence links online platforms and related systems to these vulnerabilities through three main pathways, namely excessive or displaced use driven by platform design, harmful content, and -interactions ([152],[153]).

A recent study found that social media use was associated with an increase in ADHD-related symptoms in children over time ([154]). Beyond time spent online, adverse experiences in digital spaces matter too. Online victimisation, including cyberbullying, has been associated with

[143] Bozzola, E., et al., 'The use of social media in children and adolescents: Scoping review on the potential risks', *International Journal of Environmental Research and Public Health*, 19, 2022.
[144] Vanherle, R., Hendriks, H., Beullens, K., 'Only for Friends, Definitely Not for Parents: Adolescents' Sharing of Alcohol References on Social Media Features', *Mass Communication and Society*, 26(1), 2023, pp.47–73.
[145] Geusens, F., Beullens, K., 'Triple spirals? A three-wave panel study on the longitudinal associations between social media use and young individuals' alcohol consumption', *Media Psychology*, 24(6), 2021, pp.766–791.
[146] Internet Watch Foundation, *Annual Data & Insights Report 2025*, 2025.
[147] WeProtect Global Alliance, Global Threat Assessment, 2021 as mentioned in Impact Assessment CSAR.
[148] National Center for Missing & Exploited Children, *2025 NCMEC Our Impact*, 2025.
[149] Europol, *EU Terrorism Situation and Trend Report*, 2025.
[150] World Health Organization, *Mental health of adolescents*, 2025.
[151] European Commission, *Eurobarometer 530: Mental Health*, 2023.
[152] Beullens, K., et al., 'Minors' health and social media: an interdisciplinary scientific perspective', Manolios, S., Sala, A., Sundorph, E., Chaudron, S., Gomez, E. (editors), Publications Office of the European Union, Luxembourg, 2025, p.8. [Beullens, K. et al.]
[153] Vidal, C., et al., 'Social media use and depression in adolescents: A scoping review', *International Review of Psychiatry*, 32(3), 2020, pp. 235-253.
[154] Nivins et al., 'Digital Media, Genetics and Risk for ADHD Symptoms in Children – A Longitudinal Study', *Pediatrics Open Science*, 2025.

deliberate self-harm and suicidal ideation ([155]), and cyberbullying more broadly is linked to a range of emotional difficulties, including persistent sadness, social isolation and heightened anxiety ([156],[157]). Eurobarometer data further indicate that nearly one in three adolescents report feeling stressed, sad or socially excluded because of social media, with social comparison and fear of missing out identified among the main resources of pressure ([158],[159]). These effects, however, are not uniform. They vary across services, design features and individual circumstances ([160]).

These patterns of intensive digital engagement are also associated with physical health impacts. Based on self-reports covering 30 days before the survey, children report symptoms including tired eyes, fatigue, headaches, concentration difficulties and sleep problems, with prevalence rising sharply among the heaviest screen users ([161]). More broadly, excessive or inappropriate use of digital services and systems may contribute to reduced physical activity, less time spent outdoors, and shorter or poorer-quality sleep, including by displacing sleep, increasing psychological stimulation, and suppressing melatonin production ([162]).

2.2.2. Age specific challenges

As emphasised by the Report of the Co-Chairs of the Special Panel and as illustrated by Figure 3, the **risks minors face online evolve across developmental stages,** shaped patterns of exposure, interaction and vulnerability. Available evidence indicates that **early digital exposure may have long-term impact on mental health and well-being**. Receiving a smartphone early in life has been associated with a higher likelihood of severe mental health difficulties in early adulthood, with early social media access, cyberbullying and poor-quality offline relationships as relevant mediating pathways ([163]). This is especially significant because childhood and early adolescence coincide with stages in which cognitive control, emotional regulation and resistance to social pressure remain under development ([164],[165]), with heightened

[155] Nesi, J., et al., 'Social Media Use and Self Injurious Thoughts and Behaviors: A Systematic Review and Meta-Analysis', *Clinical Psychology Review*, 8;87, 2022.
[156] Cyberbullying report.
[157] A 2015 systematic scoping review of 36 studies found a consistent association between cyberbullying via social media and depression among children and adolescents: Hamm, M. P., et al., 'Prevalence and Effect of Cyberbullying on Children and Young People: A Scoping Review of Social Media Studies'*, JAMA Pediatrics*, 169(8), 2015, pp. 770–777.
[158] Sala et al.
[159] Flash Eurobarometer FL579.
[160] European Parliament, *Mental health of young people in a digital era: Cost of non-Europe report,* 2026.
[161] Flash Eurobarometer FL579.
[162] Fegert and Melchior, pp.60-62.
[163] Thiagarajan, T. C., Newson, J. J., & Swaminathan, S., 'Protecting the Developing Mind in a Digital Age: A Global Policy Imperative', *Journal of Human Development and Capabilities*, *26*(3), 2025, pp.493–504.
[164] Steinberg, L. D., 'Age of opportunity: Lessons from the new science of adolescence', Houghton Mifflin Harcourt, 2014.
[165] Casey, B. J., Getz, S., Galvan, A., 'The adolescent brain', *Developmental review*, 28(1), 2008, pp.62-77.

vulnerability persisting well into adolescence, as reward sensitivity and concern with social evaluation intensify while these capacities are still maturing ([166],[167],[168],[169],[170]).

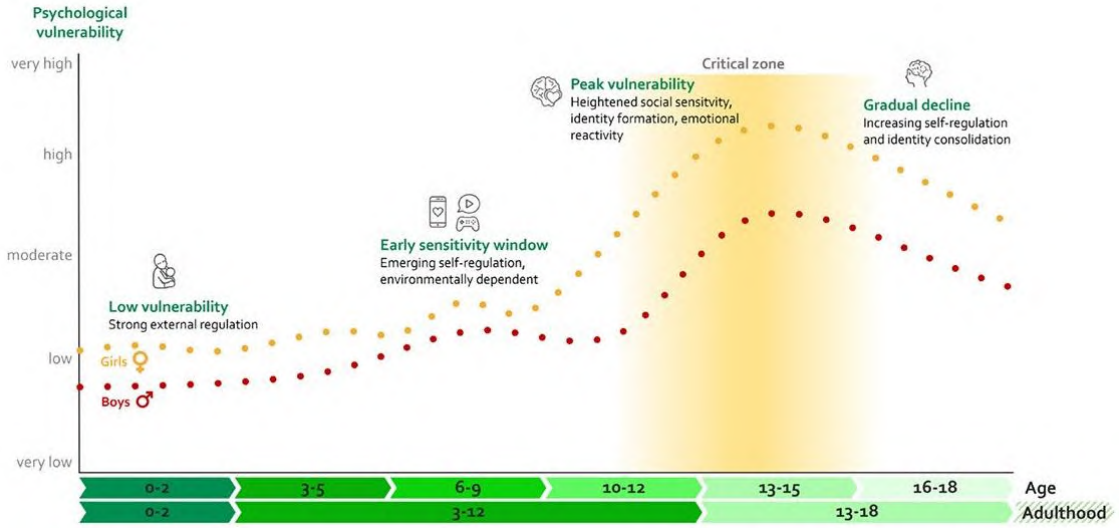


Figure 3 Psychological vulnerability throughout development.
Source: Taken from the Report of the Co-Chairs of the Special Panel([171]).

2.2.3. The emergence of new risks from AI

These developmental vulnerabilities are increasingly compounded by the growing integration of AI into children's digital lives. While AI may provide significant benefits for minors, including by supporting their development and education and by facilitating access to information, age-appropriate services and personalised learning opportunities, minors may be more susceptible to harms arising from their interactions with AI than adults, due to their age, maturity and stage of cognitive, emotional and social development. In particular, minors may have a more limited capacity to critically assess the accuracy, reliability and underlying intentions of AI-generated content and interactions, and may therefore be more likely to rely on advice or recommendations provided by AI, or to develop excessive reliance or dependency on such systems and models. Such risks are further heightened where those systems and models simulate social relationships, provide personalised or adaptive interactions, operate persistently or in emotionally salient contexts.

AI companions and chatbots are increasingly used by minors to establish such interpersonal or social interactions that may substitute healthy social and trusted relationships with other

[166] Schwartz, D., et al., 'Are social media use and popularity in the peer group linked during adolescence? A meta-analytic review', *Journal of Adolescence*, 97(3), 2025, pp.575-592.
[167] Madigan, S. et al., 'Association between screen time and children's performance on a developmental screening test', *JAMA pediatrics*, 173(3), 2019, pp.244-250.
[168] Teague, S., et al., 'Digital Media Use and Child Health and Development', *Deakin University, Journal contribution*, 2026. [Teague et al.]
[169] Yang, C. C., Holden, S. M., Ariati, J., 'Social media and psychological well-being among youth: The multidimensional model of social media use', *Clinical child and family psychology review*, 24(3), 2021, pp.631-650.
[170] Vasconcellos, R. P., et al., 'Electronic screen use and children's socioemotional problems: A systematic review and meta-analysis of longitudinal studies', *Psychological Bulletin*, 151(5), 2025, pp.513–543.
[171] Fegert and Melchior, p.43.

humans ([172],[173],[174],[175]). Particularly serious risks arise when minors are exposed to illegal, sexualised, violent or otherwise age-inappropriate or harmful content generated by those AI chatbots, including sexualised and romantic conversations, that may distort minors' understanding of relationships, intimacy, consent and appropriate sexual behaviour, creating gender-biased, unrealistic or harmful expectations about interpersonal relationships and interactions; when minors have interactions relating to self-harm or suicide; or in the context of the provision of other harmful advice minors may obtain and exposure to content that may encourage self-harm ([176], [177]). The use of such chatbots may also give rise to potentially serious risks of minors' emotional dependency, social withdrawal, and a reduced engagement in real-life relationships, as well as adverse impact on their safety, physical, emotional and mental well-being and interference with their development of independent judgement, cognitive capacities and social skills. AI chatbots may be designed or optimised to please users, agree with them, or mirror their views and emotions. For minors, this can reinforce immature, risky, or harmful beliefs and behaviours instead of challenging them appropriately.

These chatbots may also exploit vulnerabilities with manipulative design such as behavioural nudging, exploiting children's curiosity, reward sensitivity, and impulsivity ([178]). This can lead to compulsive use, with adolescents spending hours each day interacting with AI at the expense of schoolwork and real-world relationships, diminished autonomy and, in several cases, emotional distress when access is restricted or the system is altered ([179]). Moreover, biases embedded in AI systems, including algorithmic and societal ones, may further amplify the spread of harmful content and misinformation, entrenching stereotypes that children can internalise from an early age ([180]).

2.2.4. Specific risks on online games

Estimates show that ~80% of minors between 2 and 18 spend 30% of entertainment time gaming ([181]). While playing online games, minors can find entertainment, environments to connect, communicate and share as well as other benefits such as finding community and

[172] Hudon, A., Stip, E. 'Delusional Experiences Emerging From AI Chatbot Interactions or "AI Psychosis"', *JMIR Mental Health*, 3 (12), 2025.
[173] European Parliamentary Research Service (EPRS), *The spread of AI companions and the challenges they generate*, 2026.
[174] Nature, *Can AI chatbots trigger psychosis? What the science says*, 2025.
[175] Yu et al., 'Understanding Generative AI Risks for Youth: A Taxonomy Based on Empirical Data', *University of Illinois Urbana-Champaign*, 2025. [Yu et al.]
[176] Vice, 'He Would Still Be Here': Man Dies by Suicide After Talking with AI Chatbot, Widow Says', 2023.
[177] Branch, J. B., 'AI Companions Are Not Your Teen's Friend', *Issues in Science and Technology* 42.1, 2025, pp.80-83.
[178] Kurian, N., 'AI's empathy gap: the risks of conversational artificial intelligence for young children's well-being and key ethical considerations for early childhood education and care', *Contemporary Issues in Early Childhood*, 26(1), 2023, pp.132-139.
[179] Yu et al.: The study distinguishes two dimensions of over-reliance. Reduced autonomy refers to a diminished capacity for independent thinking and decision-making, as minors increasingly default to the GAI system for schoolwork, personal advice or emotional regulation rather than developing these skills themselves. Emotional distress refers to cases where minors, having formed a strong attachment to a specific AI companion, experience acute reactions such as feelings of loss or self-harm when that companion becomes unavailable or unrecognisable, for instance following a platform ban, an account suspension or a company-driven update to the underlying model.
[180] Weninger, O., 'The algorithm babysitter: AI-generated content and the emerging human rights crisis in early childhood, *Human Rights Research*, 2025.
[181] European Commission, *The European media industry outlook – September 2025*, 2025, p. 88, note 322. [European media industry outlook]

escaping stress or negative feelings ([182],[183]). A wide variety of online games exist, which differ in type and business model, with many also offer features resembling online platforms and posing similar risks ([184]). Open communication and the creation of user-generated content on these services may expose children to cyberbullying, grooming, radicalisation or age-inappropriate content ([185]). Certain games may also use specific commercial practices that can exploit the vulnerability of children and cause unwanted spending, compulsive or addictive behaviours, such as loot boxes, pay-to-advance mechanisms and certain in-app purchases and virtual currencies ([186],[187],[188]). Additionally, gaming disorder is now included in the WHO International Classification of Diseases, with evidence suggesting that boys between 11 and 15 face heightened risk of problematic use and affect adolescents facing possible behavioural and emotional issues as well as psychosocial and sleep-related disturbs ([189]).

2.2.5. The benefits of the online environment

Despite exposure to a wide range of risks, **digital services and systems also offer important opportunities for minors.** For many children and young people, the digital sphere offers spaces for participation, social connection and community-building, including for those who may feel marginalised or isolated offline ([190]). Social media and other digital services and systems can facilitate peer affirmation and relationship-building and may help reduce feelings of loneliness where in-person interaction is restricted ([191],[192],[193]), while also providing relatively low-pressure environments for identity development, self-expression and creative exploration ([194],[195]).

Digital services and systems can also function as an important source of information and support, particularly for vulnerable minors looking to connect with others who share similar

[182] Schlegel, L., Playing Against Radicalization: Why extremists are gaming and how P/CVE can leverage the positive effects of video games to prevent radicalization, 2022.
[183] European Commission, *Understanding the value of a European video games society*, 2023.
[184] European media industry outlook: Games increasingly function as social and multi-purpose digital spaces, not just entertainment products: among people using games such as Fortnite, Roblox or Minecraft, 40% consume additional media content within the game platform, and 33% follow classes or use games as learning support, particularly young adults.
[185] Radicalisation Awareness Network, *Digital Grooming Tactics on Video Gaming & Video Gaming Adjacent Platforms: Threats and Opportunities – Conclusion paper*, 2021.
[186] Cfr. Brooks, G.A., Clark, L., 'Associations between loot box use, problematic gaming and gambling, and gambling-related cognitions', *Addictive Behaviors*, 96, 2019.
[187] BEUC, *Game Over: A legal assessment of premium in-game currencies from a consumer law perspective*, 2024.
[188] Forbrukerrådet (the Norwegian Consumer Council), *GET PLAYED: The true cost of virtual currency*, 2024.
[189] Boniel-Nissim, M., et al., *A focus on adolescent social media use and gaming in Europe, central Asia and Canada. Health Behaviour in School-aged Children international report from the 2021/2022 survey: Volume 6*. WHO Regional Office for Europe, 2024.
[190] Flash Eurobarometer FL579: Nearly half of young people (48%) report that their online activities have a positive effect on their mental wellbeing, with connection (70%), learning (65%) and entertainment (57%) identified as the main reasons.
[191] Popat, A., Tarrant, C., 'Exploring adolescents' perspectives on social media and mental health and well-being A qualitative literature review', *Clinical Child Psychology and Psychiatry*, 28(1), 2023, pp.323-337. [Popat and Tarrant]
[192] Singleton, A., Abeles, P., Smith, I.C., 'Online social networking and psychological experiences: The perceptions of young people with mental health difficulties', *Computers in Human Behavior*, vol. 6., 2016. [Singleton et al.]
[193] Sala et al.
[194] Some minors may use private social media accounts as a digital equivalent of offline journaling: *Ibid*.
[195] A 2022 survey of 1,316 adolescents in the United States reported that 71% regarded social media as a platform for expressing their creativity. Source: Anderson, M., Vogels, E.A., Perrin, A., Lee, R., *Connection, Creativity and Drama: Teen Life on Social Media in 2022*, Pew Research Centre, 2022.

experiences ([196],[197]). For instance, research indicates that adolescents from LGBTQI+ communities may be more inclined to use online environments to explore their sexuality and identity, access information on sexual health, and seek peer support and social connection while avoiding the risks associated with "in-person" interactions.

In addition, digital tools can enhance learning and skills development through more personalised and engaging forms of instruction ([198],[199],[200],[201]), while AI-based applications can further expand opportunities for tailored support and feedback. This enables educators to adapt teaching to student performance, provide timely feedback and support, and tailor individual assistance accordingly ([202],[203]). **Realising these benefits, however, depends on minors being able to interact safely online, which is why services and systems should be safe by design.**

2.2.6. Age-inappropriate platform design

Platform design is central to both the risks outlined above and the extent to which minors can safely realise the benefits digital services offer ([204], [205]). This is illustrated by the Online Minor Protection Matrix developed by the European Commission's Joint Research Centre, which maps common platform features, including recommender systems, default settings, notifications and beauty filters, onto the categories of risk with which they are most commonly associated ([206]). These features are not inherently risky; their impact depends on platform design and use. Some, such as parental controls, are generally protective, while others, such as beauty

[196] A commonly articulated view among minors is that online spaces constitute comparatively 'safe' avenues for self-expression and more accessible sources of support than 'traditional' alternatives, such as seeking guidance from parents or counsellors. Source: Shankleman, M., Hammond, L., Jones, F.W., 'Adolescent Social Media Use and Well-Being: A Systematic Review and Thematic Meta-synthesis', *Adolescent Research Review*, vol. 6, 2021.
[197] Popat and Tarrant; Singleton et al. For instance, moderated forums have helped some adolescents address their hesitation about seeking professional support.
[198] Forsström, S., et al., 'Key findings and integration strategies on the impact of digital technologies on students' learning: Results from a literature review', OECD Education Working Paper No. 336, 2025. [Forsström et al.]; In disciplines such as science, mathematics, and languages, digital technologies may enhance learning by providing interactive pedagogical experiences, including simulations, modelling tools, animations, digital games, multimedia resources, and audio elements. Such approaches can foster student engagement and render abstract or complex concepts more accessible and comprehensible.
[199] Barrot, J.S., 'Social media as a language learning environment: A systematic review of the literature (2008-2019)', *Computer Assisted Language Learning*, 35 (9), 2022.
[200] Zachos, G., Paraskevopoulou-Kollia, E.-A., Anagnostopoulos, I., 'Social Media Use in Higher Education: A Review', *Education Sciences*, 8 (4), Article 4, 2018.
[201] Digital technologies provide educators and learners with additional opportunities for teaching and learning, and are most effective when used to complement rather than replace traditional pedagogical approaches. Source: Hillmayr, D., et al., 'The potential of digital tools to enhance mathematics and science learning in secondary schools: A context-specific meta-analysis, *Computers & Education*, vol. 153, 2020.
[202] Villar Onrubia, D., et al., *Generative Artificial Intelligence in secondary education – Uses and perceptions from the perspective of early adopters across five EU Member States*, Luxembourg, JRC144345, 2025.
[203] Forsström et al.
[204] Sala et al.
[205] van der Wal, A.,et al, 'Diverse platforms, diverse effects: Evidence from a 100-day study on social media and adolescent mental health', *Curr Psychol*, 45, 36, 2025. [Van der Wal et al]. For instance, the results of van der Wal et al. suggest that "highly visual platforms share several features that may help explain their adverse effects. First, they are saturated with edited, idealized images which are known to undermine adolescents' self-esteem through upward social comparison processes (Rousseau & Rodgers, 2025). Second, these platforms' algorithmic recommender systems often amplify exposure to distressing or problematic content, particularly for vulnerable youth (Hilbert et al., 2023). Third, their engagement-maximizing design often encourages excessive use, which can displace time and attention away from activities that support well-being, self-esteem, and friendship closeness."
[206] Manolios, S., *Online Minor Protection Matrix*, Chaudron, C., Sala, A., Gomez, E. (editors), Publications Office of the European Union, Luxembourg, 2026, JRC147657.

filters, are more consistently associated with harm, and many, including comments and content recommendations, may be either beneficial or harmful depending on implementation.

Platform design choices play a key role in creating these risks, as current protection for minors remain inadequate. Addictive design features and "dark patterns", such as autoplay, infinite scrolling, gamification and push notifications, may distort minors' ability to make autonomous choices and encourage prolonged engagement ([207],[208],[209],[210],[211]). At the same time, recommender systems that rely on behavioural data to personalise content may steer minors towards harmful or age-inappropriate material, reinforcing repeated exposure and interaction ([212]). Other design elements, including "like" mechanisms, read receipts, and notifications, have likewise been identified as deliberate tools for maximising engagement ([213],[214]), reflecting the systemic risks recognised under the DSA. Emerging evidence suggest that platform design affects adolescent well-being. In a 100-day study, the use of short video platforms with engagement-maximizing feeds had overwhelmingly negative effects on well-being and self-esteem, whereas messaging-focused services showed neutral or positive effects ([215]).

2.2.7. An insufficient level of compliance and legislative gaps

Overall, the online environment has not been designed with children in mind and does not cater for their evolving capacities. Children face many risks online, which can have severe impacts on their well-being, development as well as their physical and mental health. Those risks are constantly evolving together with new technologies and platforms, as children are early adopter of new technologies, they also remain the most vulnerable to these risks. While the opportunities offered by the online environment should not be underestimated, their realisation and positive impacts on the lives of children ultimately depend upon digital services and systems being safe and age appropriate.

---

[207] European Commission, *Consumer protection: manipulative online practices found on 148 out of 399 online shops screened*, January 2023.

[208] Flayelle, M., et al., 'A taxonomy of technology design features that promote potentially addictive online behaviours', *Nature Reviews Psychology*, 2, 2023, pp.136–150. [Flayelle et al.]

[209] Comparing platforms' EU risk assessments under the DSA with internal company documents disclosed through US litigation, the Knight-Georgetown Institute found that Meta and TikTok's public risk assessments give limited consideration to how core design choices may themselves drive problematic use, while internal documents show both companies have privately classified millions of minors as exhibiting "objectively harmful" use. Source: Chapman, P., Steinberg, M., *Measuring Risk: What EU Risk Assessments and US Litigation Reveal About Meta and TikTok*, Knight-Georgetown Institute, February 2026.

[210] A comparable analysis of Snap and YouTube's EU risk assessments and internal documents disclosed through US litigation found similarly limited consideration of how design choices, including ephemeral content and features recommending adult contacts to minors, may drive problematic use and unwanted contact. Source: Knight-Georgetown Institute, *Measuring Risk 2: What EU Risk Assessments and US Litigation Reveal About Snap and YouTube*, July 2026.

[211] In March 2026, a California jury found Meta and Google liable for design choices, including infinite scroll, algorithmic recommendations and autoplay, that fostered compulsive use in a minor, awarding $6 million in damages in what was reported as the first case treating a social media platform as a defectively designed product. Source: K.G.M. v. Meta Platforms, Inc. and Google LLC, Los Angeles County Superior Court, verdict delivered 25 March 2026.

[212] Regehr, K., et al., 'Normalizing toxicity: the role of recommender algorithms for young people's mental health and social wellbeing', *Frontiers in Psychology*, *16*, 2025, 1523649.

[213] Flayelle, et al.

[214] Mildner, T., et al, 'About engaging and governing strategies: A thematic analysis of dark patterns in social networking services', *Proceedings of the 2023 CHI conference on human factors in computing systems*,2023.

[215] Van der Wal, et al.

The European Union has made the protection of minors online one of its core priorities. With the DSA, the critical role and responsibility of digital services and systems in designing a safe environment and empowering users have been recognised and enshrined in law. Article 28(1) DSA obliges providers of online platforms to put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors, on their service. With the publication of its guidelines on the protection of minors in July 2025, the Commission has further set out measures that online platforms must take to ensure a high level of privacy, safety and security. They include adapting their recommender systems, account settings, reporting systems and disabling features contributing to excessive use such as streaks, autoplay, read receipt and push notifications ([216]). In addition, VLOPs and VLOSEs must diligently identify, analyse and assess any systemic risks to the rights of the child, the protection of minors and any actual of foreseeable negative effects on physical and mental wellbeing (Article 34 DSA). Following this assessment, they must put in place effective measures to mitigate those risks, including adapting their online interfaces and recommender systems (Article 35 DSA).

Despite those established standards, there are concerns that providers continue to fall short and risks remain on online services for minors. In 2026 alone, the Commission preliminarily found both TikTok and Meta ([217],[218]) in breach of the DSA over addictive design features and inadequate safeguards for minors, opened proceedings against Snapchat over grooming and inadequate default account settings ([219]), and preliminarily found that Meta had failed to prevent minors under 13 from accessing Instagram and Facebook ([220]). To note again that Preliminary Findings and opened proceedings are only an intermediate step in a Commission investigation, and the investigation continues (for opened proceedings) or VLOPs now have the possibility to exercise their right to defence (for preliminary findings), before the Commission decides on next steps in these cases. However, these steps signal the suspicion of potential lack of compliance of these providers. Similarly, the Commission has some concerns as to the overall level of implementation of the guidelines on protection of minors across online platforms. These continued concerns indicate the need to further clarify existing rules and codify more precisely measures to ensure a safe and age-appropriate environment for minors online.

Concerning online games, section 2.2.4 highlights how some risks are present across types of games and are not only limited to online games that are online platforms. Some online games

[216] Guidelines on the protection of minors.

[217] European Commission, *Commission preliminarily finds TikTok's addictive design in breach of the Digital Services Act*, 6 February 2026 (IP/26/312). [Preliminary findings on TikTok's addictive design]. The Commission found that TikTok had disregarded indicators of compulsive use, such as time spent on the app at night and the frequency with which users opened it, and that its screen-time and parental control tools were easy to dismiss and required additional effort from parents to activate.

[218] European Commission, *Commission preliminarily finds the addictive design of Instagram and Facebook in breach of the Digital Services Act*, 10 July 2026 (IP/26/1579). This finding builds on the same investigation opened in May 2024 that produced the April 2026 findings on underage access, and runs in parallel with a separate, ongoing inquiry into the "rabbit hole" effects of Facebook's and Instagram's recommender systems on minors.

[219] European Commission, *Commission investigates Snapchat's compliance with child protection rules under the Digital Services Act*, 26 March 2026 (IP/26/723). [Snapchat opening of investigations]. The investigation, which absorbed an earlier Dutch inquiry into vape sales to minors, examines five areas: age assurance, grooming and criminal recruitment, default account settings, dissemination of illegal or age-restricted products, and the accessibility of illegal-content reporting mechanisms. The Commission suspects that adults circumvent age checks by misrepresenting their own age, allowing them to appear as minors and approach children more easily.

[220] European Commission, *Commission preliminarily finds Meta in breach of Digital Services Act for failing to prevent minors under 13 from using Instagram and Facebook*, 29 April 2026 (IP/26/920). [Preliminary findings on META for risks for under 13] According to the Commission, roughly 10-12% of children under 13 across the EU access Instagram and/or Facebook despite the platforms' minimum age requirement; Meta's tool for reporting underage users reportedly requires up to seven clicks and often results in no follow-up action.

might therefore not be covered by existing rules while presenting similar risks, indicating the need to extend the scope of safety by design obligations.

As regards AI, while the AI Act contains several safeguards to protect health, safety and fundamental rights, including those of minors, risks to minors posed by companions and chatbots are not subject to specific safety by design measures. Under the AI Act, AI chatbots and companions are subject to the transparency requirements for AI systems directly interacting with natural persons and to the requirement to mark AI-generated content to enable its detection. Depending on other functionalities and factors, an AI companion may also constitute a prohibited practice (for example, in cases involving the exploitation of children's vulnerabilities) or qualify as a high-risk AI system (for instance, where it incorporates emotion recognition functionalities). The Commission monitors the risks these systems can pose and has noted this as an area of concern in its report published as required under Article 112(1) AI Act ([221]).

The current framework does not comprehensively address risks arising from AI companions and general conversational chatbots that, although not classified as high-risk AI systems, are likely to be used by or to interact with minors in everyday contexts causing risk to minors' health, safety and fundamental rights and their well-being and development, as explained in the previous sections. Such risks vary from possible addictive designs in AI chatbots to AI features capable of displaying behaviours or simulating emotions or interpersonal relationships that may lead to emotional dependencies for minors and other physical, mental and emotional well-being and developmental concerns ([222]).

As the risks facing minors online remain high and severe, a strengthened framework must be established to ensure that digital services and systems providers adopt the necessary measures for minors as a matter of emergency. This new legislation will take the child as the starting point and enshrine the need for safety by design and age-appropriate measures across the digital environment. Clarifying and codifying rules on minimum age for certain services and systems as well as on safety by design will ease compliance and enforcement, as well as clearly put the responsibility onto the providers of those services and systems to demonstrate that their service or system is safe.

2.3. A lack of clear requirements for age assurance and ineffective implementation

To ensure a safe and age-appropriate online environment for minors, age assurance is critical as noted by the Report of the Co-chairs of the Special Panel. Indeed, age assurance underpins both age restrictions and age-appropriate safety by design measures. However, the current framework around age assurance lacks clarity and its implementation is patchy.

2.3.1. Age assurance underpins safe online experiences for minors

Age assurance is crucial to ensure that minors only access services and systems that are safe and age appropriate. Currently, many minors below the established age limit access and use digital services and systems that are not designed for them. A range of surveys indicate that in the EU millions of minors under the age of 13 use social media and have their own accounts

[221] Report from the Commission to the European Parliament and the Council, Report adopted pursuant to Article 112(1) of Regulation (EU) 2024/1689 on the need to review the list of prohibited AI practices and of high-risk AI systems listed in Annex III (COM(2026) 234 final).
[222] Negreiro, M. and Anaç, Ö. D., *The spread of AI companions and the challenges they generate*, European Parliamentary Research Service, 2026.

([223]). For example, across six countries, 34% of 9–11-year-olds report having a social media profile ([224]). In April 2026, the Commission preliminary found META in breach of the DSA for failing to effectively prevent minors under 13 from accessing Instagram and Facebook ([225]). The measures put in place by META to enforce the restrictions of 13 do not seem to be effective. The Commission also investigates TikTok and Snapchat for the same issue ([226]). To note again that Preliminary Findings and opened proceedings are only an intermediate step in a Commission investigation and merely indicate a suspicion of a potential lack of compliance of these providers.

Age assurance is also important to ensure that minors who are old enough to have accounts receive age-appropriate experiences. The Report of the Co-Chairs of the Special Panel emphasizes that child safety online must follow a developmental approach that tackles age-specific risks. Some online services have started – to an extent – to differentiate certain experiences for different age groups. For instance, several services now offer so-called "teen accounts", and the terms and conditions of certain platforms only allow users above 16 or above 18 to host LIVE streams or to access adult content, and vary some account settings with age ([227], [228]). While the account settings on many online services are often not safe for minors even when the platforms identify them as such ([229]), minors automatically receive adult settings when they are not recognised as minors. The guidelines on the protection of minors make clear that ineffective age assurance such as self-declaration alone measures cannot underpin age-appropriate design. As mentioned above, the Commission investigates several very large online platforms for failing to ensure that 13-17-year-olds receive age-appropriate experiences ([230], [231]), indicating a suspicion of potential lack of compliance of these providers.

2.3.2. Ineffective implementation of age assurance

Existing age requirements on online services are typically not developed based on children's needs and hardly enforced. Most providers of digital services set out a minimum age to access or use their service in their terms and conditions ([232]). As noted by the OECD, the rationales behind the ages chosen by services derive from privacy and contract laws reasons rather than

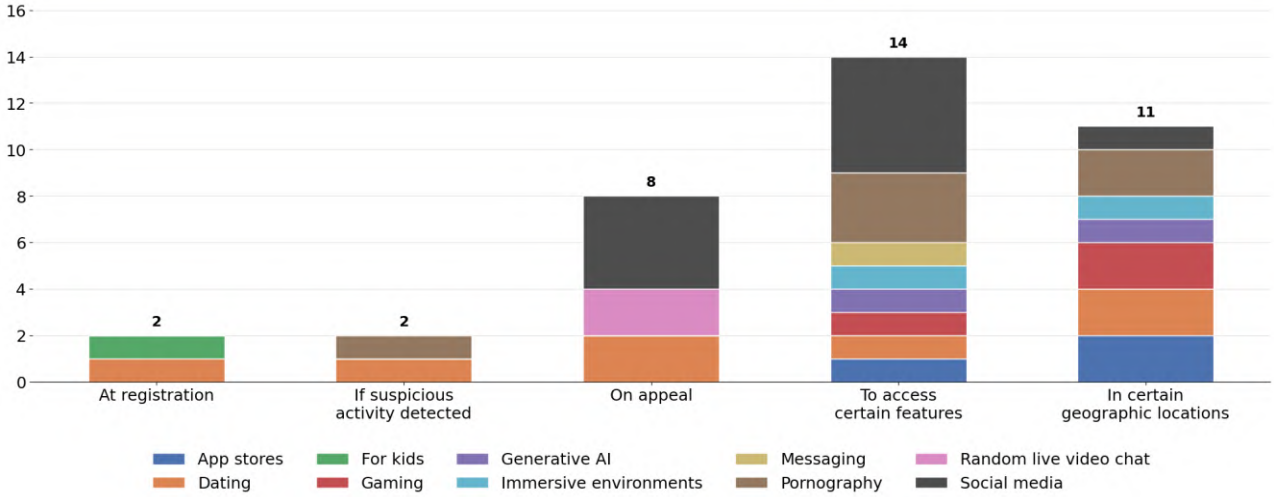
[223] A 2025 survey among adolescents in Belgium, Italy, Poland, Portugal, and Spain finds that most minors started using social media before the age of 13. Many 12-year-olds have own their own social media accounts. For example 66% report having their own YouTube account, 47% their own Instagram account, 45% their own TikTok Account, 28% their own Snapchat account, 13% their own Twitter account (Euroconsumers Group, *Growing up online Building a digital-future for minors by minors*, 2025.) Surveys from a wide range of MS confirm that many U13 minors have social media accounts. Surveys outside the EU find similar results. For instance, Ofcom finds in the UK that "[a] majority of children under 13 had their own profile on at least one social media app or site; 33% of parents of 5-7s said their child had a profile, and 60% of 8-11s said they had one." (Ofcom, *Children and parents: Media use and attitudes report 2022*).
[224] EU Kids Online 2026.
[225] It is important to note that those preliminary findings to not prejudge a finding of compliance or non-compliance, [Preliminary findings on META for risks for under 13].
[226] European Commission, *Commission opens formal proceedings against TikTok under the Digital Services Act*, 19 February 2024 (IP/24/926) [Opening of proceedings against TikTok], and [Snapchat opening of investigations].
[227] OECD, 2025, *Age assurance practices of 50 online services used by children*, OECD Publishing, Paris, 2025. [OECD]
[228] Ofcom, *Report on the Use of Age Assurance*, 2026. [Ofcom age assurance report]
[229] Trell, N., *Private by Default, Protected by Design? An In-Depth Comparative Assessment of Four Platforms under the DSA Article 28(4) Guidelines*, DSA-Monitor. Österreichisches Institut für angewandte Telekommunikation, 2026.
[230] Opening of proceedings against TikTok.
[231] Snapchat opening of investigations.
[232] OECD.

based on an assessment of safety or developmental appropriateness ([233]). The OECD further highlights that "very few of [the services that set a minimum age in their Terms of Service] implement age assurance in a systematic way" and that only 2 out of the 50 online services studied systematically require assure age for account creation ([234]). The only age check before account creation is typically self-declaration. It is widely recognised that self-declaration alone is not an effective age assurance measure, because many users do not reveal their true age ([235], [236], [237]). Minors routinely mis-state their age online ([238]). In practice, underage users can therefore easily access many age-restricted online services.

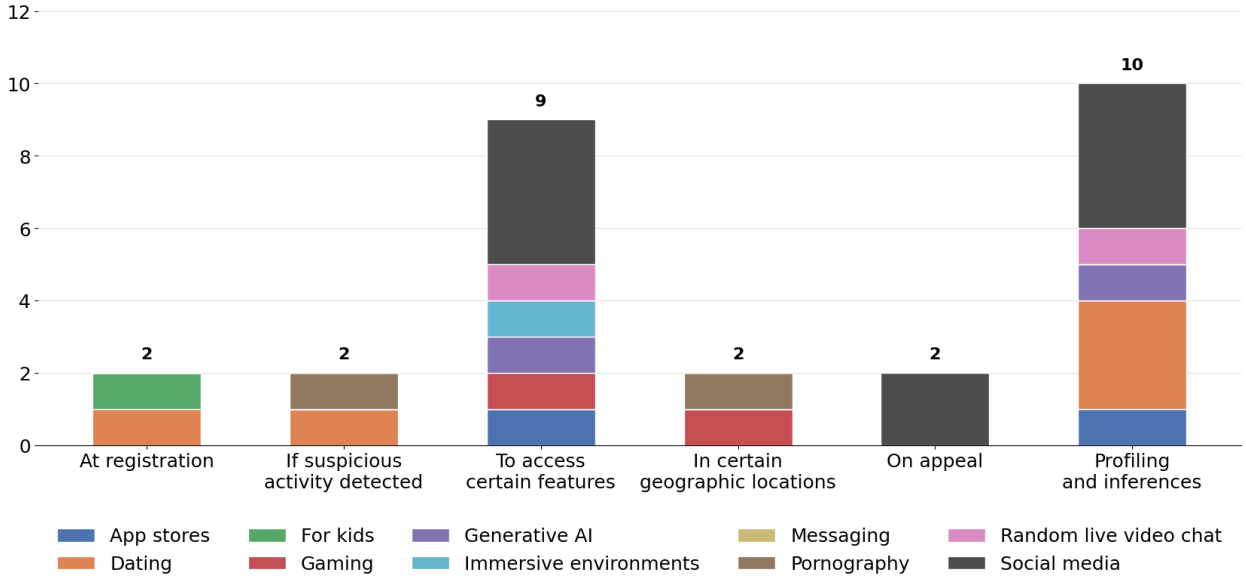
Figure 4 illustrates that both age verification and age estimation are deployed at most in haphazard way. Some services have recently started to require age checks before accessing certain high-risk features, such as live streams. Yet, many users do not use these features and users typically remain on the service if they fail to prove being old enough for an age-restricted feature. Hence, most users only need to prove their age once they have been flagged as likely underage and offered to appeal a pending account suspension. Account-based services often try to infer users' age ex post, for instance by using age inference models that predict users age from their behaviour on the service (behavioural profiling), sometimes combined with human reviews ([239]). While these systems can contribute to age assurance, they have failed to detect many minors with false stated ages. This is likely due both to inherent limitations of age inference – especially for users who reveal limited information about themselves and do not share videos and images of themselves – and to implementation choices that reduce the detection of minors ([240]).

[233] *Ibid*.
[234] *Ibid*.
[235] Shaffique, M. R., van der Hof, S, *Mapping Age Assurance Typologies and Requirements: Research Report*, Publications Office of the European Union, 2024. [Shaffique and van der Hof]
[236] Rescorla, E., Arnao, Z., Cooper, A., *Age Assurance Online: A Technical Assessment of Current Systems and Their Limitations*, 2026. [Rescorla et al.]
[237] Collins, S., *Getting Age Assurance Right: a Risk-based framework for high-risk online features*, Public Knowledge, 2026.
[238] For example, a Danish study found that 71 % of minors between 13 and 17 indicated that they had at some point lied about their age to access a website, create a profile, or download an app. A study conducted in Spain by UNICEF Spain shows that 44 % of minors aged between 9 and 16 mis state their age when creating a profile on social networks, while only 40 % of respondents claim to declare their real age. An Ofcom study finds that nearly half of 8–17-year-olds said they set up their profile on most platforms without using their actual date of birth (Ofcom, 2022. Children's Online User Ages Quantitative Research Study). In a survey among 1,000 Dutch school children aged 10 to 16, 99% of report providing a different age.
[239] See, for instance, OECD; Rescorla et al.
[240] See, for example, Ofcom age assurance report; Rescorla et al.and the PIPEDA Findings #2025-003 by the Office of the Privacy Commissioner of Canada.

Figure 4 Circumstances in which online services use (a) age verification and (b) age estimation in 2024



(a) *Use of age verification*



(b) Use of age estimation

Note: Taken and adapted from OECD (2025).[241]

The recent experience in Australia illustrates that it is difficult to ensure effective age assurance without concrete requirements for age checks before account creation. The Australian law only requires "reasonable steps to prevent Australians under 16 from creating or keeping accounts" ([242]). A range of surveys and the eSafety Commissioners own data suggest that the majority of

[241] OECD; In interpreting the figure, it should be noted that the ten service categories above are a non-exhaustive selection of different types of online services used by children, and that each service is included in only one category even though those categories are not mutually exclusive. For example, a service could provide both gaming and immersive environments. Therefore, absolute numbers should be treated with caution.

[242] eSafety Compliance Update 2026

minors who previously had social media accounts still have them ([243],[244],[245],[246]). Crucially, most minors were never asked to prove their age ([247]). More recent laws on online age restriction typically require age checks before account creation ([248]). While no age assurance system is completely circumvention-proof, age checks before account creation likely increase the effectiveness of age restrictions.

2.3.3. The need for clear age assurance requirements

While age assurance is an important measure to ensure the safety of children online, they should not result in the exploitation of users' personal data. Many services currently do no offer users any privacy-preserving options to verify their age. Some services force users to upload their identity documents directly to the service ([249]). This creates significant privacy and security risks because it reveals the user's identity and often additional sensitive information on the document, such as precise birthdate, national identity number, sex, home address, and sometimes other personal characteristics ([250]). Furthermore, these data are sometimes stored for extended periods of time ([251]). As emphasized by Fegert and Melchior (2026), "[a]ny method employed to check age should uphold the highest privacy and data protection standards and should not lead to the processing of identity documents and biometric data for the purpose of age estimation." Privacy-preserving age assurance solutions are rapidly developing, and the EU Age Verification Solution allows citizens to verify their age under the highest privacy standards ([252]). In order to be implemented in such a way that they always remain privacy-preserving, such solutions must be mandated to respect minimum requirements, so as to ensure that age assurance measures remain in line with the fundamental rights of all users, including their right to privacy and data protection.

Overall, age assurance is an important measure for the protection of minors online, not only in terms of enforcing access restrictions to content or services that are harmful to children, but also to ensure that services are designed in an age-appropriate manner. Currently, age assurance measures are not robust nor effective and are used in a manner that may infringe upon children and adult's rights to privacy and data protection. Clear rules are therefore necessary so that age assurance is used in a manner that serves minors in practice, is proportionate to the risk and abides by fundamental rights.

3. PROPOSED REGULATION: A HARMONISED APPROACH TO CHILDREN'S ONLINE SAFETY

Considering the fragmentation of the internal market, the currently insufficient level of compliance and protection for minors online and the ineffective implementation of age

[243] *Ibid.*
[244] Barnes, C., et al., 'Assessing early effects of Australia's Social Media Minimum Age Act on adolescents' social media use: observational study'; *BMJ* 393, 2026.
[245] Bursztyn, L., et al., 'Why bans fail: Tipping points and Australia's social media ban', *BFI Working Paper No. 2026-57*. [Bursztyn et al.]
[246] Molly Rose Foundation, 2026, *Australia's social media ban – is it working?*, 2026
[247] *Ibid* (supra164 and 165).
[248] See, for example, the UK National consultation, the proposal of the Canadian Safe Social Media Act, and Indonesia's Regulation No. 9.
[249] See OECD. ID uploads are common across a range of online services, including, among others, app stores, social media and dating apps.
[250] Rescorla, E., Arnao, Z., Cooper, A., *Age Assurance Online: A Technical Assessment of Current Systems and Their Limitations*, 2026.
[251] Meta, for instance, stores an encrypted copy of the ID document for 30 days; see META, *Learn about ID verification for META accounts*, accessed July 2026.
[252] Winecoff, A.; Cooper, A, *Age Assurance Rules An Implementation Guide*, Knight-Georgetown Institute, 2026.

assurance, a new legislative instrument is required to harmonise rules on access delays, strengthen the level of protection of minors online and provide clear criteria on the use of age assurance.

3.1. The need for a harmonised European approach

Following on the Report of the Co-Chairs of the Special Panel, this new legislative instrument aims to further improve the protection of minors in the online environment, and ensure the functioning of the single market, in particular in relation to the cross-border provision of certain online services and systems. The legal basis for the proposed Regulation is Article 114 of the Treaty on the Functioning of the European Union (TFEU) ([253]). In accordance with Article 114(3) TFEU, the proposed Regulation aims at ensuring a high level of protection for the health and safety of children across the Union considering new technological developments.

As noted by the Report, and as demonstrated in section 2.1, harmonised rules at Union level establishing a single legislative framework for providers of certain online services and systems accessible to minors would contribute to the proper functioning of the single market by simplifying the legal environment for providers of those services and systems, ensuring legal certainty and easing compliance.

Considering the significant risks faced by children online across the Union and the cross-border aspect of certain digital services and systems, the proposed Regulation will provide a common, clear and coherent legal framework for the protection of minors in the digital environment. By taking children and their specific needs as a starting point, the proposed Regulation will further complement the DSA and the AI Act ensuring legal certainty and a high level of protection for minors online. Children will benefit from the same level of protection across the Union.

By setting clear rules on protection of minors online, the proposed Regulation also aims at providing for the best conditions for innovative cross-border digital services and systems to develop in the European Union, in respect of children's needs and evolving capacities.

3.2. A regulation for child online safety

In line with the recommendations of the Co-Chairs of the Special Panel, the proposed Regulation aims at ensuring a strong and coherent framework for the protection of minors online. The proposed Regulation will have the objective to (1) protect minors from being exposed to an age-inappropriate experience online, (2) ensure the respect of the rights of the child in the online environment, (3) uphold the digital single market; and (4) maintain a coherent regulatory framework and enforcement structure for the protection of minors online.

In line with those overall objectives, the proposed Regulation therefore sets out the following:

(a) Provide for a harmonised minimum age of 15 years for creating an account on risky social networking services and video-sharing platforms;

(b) Provide for the possibility, under certain conditions, for guardians to create accounts for minors below 15 with certain services and systems that fulfil safety requirements and allow access through such accounts with parental supervision;

[253] Consolidated version of the Treaty on the Functioning of the European Union (C 326/47).

(c) Provide harmonised safety by design requirements for services and systems in scope;

(d) Establish clear requirements and criteria for the use of age assurance systems to underpin the access delay and the implementation of safety by design measures;

(e) Encourage and provide guidance to Member States on developing national measures and policies to support and complement the proposed Regulation;

(f) Consolidate a coherent and robust enforcement framework to ensure timely and efficient implementation.

The sections below set out how the proposed Regulation will address each of these elements. Additionally, section 3.2.6 analyses how the proposed Regulation addresses the recommendations of the Co-Chairs of the Special Panel.

3.2.1. Provide for a harmonised minimum age of 15 years for creating an account on risky social networking services and video-sharing platforms

As outlined in the Report of the Co-Chairs of the Special Panel, and in section 2.2, certain online social media are particularly risky for minors and access to such services shall be delayed. A harmonised minimum age would ensure a uniform and high level of protection for all children across the EU on these services and systems. In line with children's fundamental rights to freedom of expression and information, the proposed Regulation delays access only to the creation of accounts on defined categories of services, online social networking services and video-sharing platform services, that pose specific risks to minors based on their functionalities as listed under Article 6(1) of the proposal. Those functionalities aim at targeting specifically addictive or compulsive use, contacts risks, conduct risks and content risks. For instance, limiting contact and the sharing of content with strangers aims at reducing risks of grooming and child sexual abuse as offenders systematically use social media to establish contact with minors ([254]).

To further ensure the proportionality of the access delay, the scope of the proposed Regulation does not apply to certain services and systems, such as not-for-profit encyclopaedias, services and systems designed for purely educational purposes and operated by educational establishments, services and systems designed and operated for purely scientific purposes, and open-source software development platforms. In addition, the proposed Regulation also foresees the possibility of amending this list with a view to exempt other services or systems that may pose equivalently low or lower risks to minors as these categories of services and systems.

While the Report of the Co-Chairs of the Special Panel recommended a harmonised EU-wide access restriction for children under 13, the proposed Regulation delays the possibility to create an account on risky services and systems in scope until the age of 15 in view of the specific vulnerabilities of adolescents between 13-15 as pointed out in the same Report. Until 15 years old, teenagers are vulnerable to social evaluation, more prone to risk-taking and are developing their cognitive control systems. Social media and other risky services and systems can reinforce dependence on external regulation in a time where adolescents are extremely vulnerable to mental health problems ([255]). To limit their exposure to potential harm during a stage of peak

[254] Fegert and Melchior, p.64.
[255] *Ibid*, p.45.

developmental vulnerability, autonomous access to social networking and video-sharing platforms should be delayed.

3.2.2. Provide for the possibility for children below 15 to access certain services and systems that fulfil safety requirements with parental supervision

As recognised by the Report of the Co-Chairs of the Special Panel, children are not a homogeneous group considering their personal and individual circumstances ([256]). Children may be at different stages of development and maturity while of the same age. In this context, it is important to consider that risks of addiction emerge from the interaction between digital features, such as variable rewards, infinite scrolling and constant availability, and developmental vulnerabilities. Moreover, parents have a special role in guiding their children in accessing and using the digital world and remain best placed to assess their children's needs and vulnerabilities.

To facilitate the child's transition to autonomy, and in line with its best interest ([257]), guardians will have the possibility to set up an account for their children between the age of 13-15 with limited functionalities. Furthermore, for children below 13, guardians may decide to give guardian-controlled access to their children to child-friendly video-sharing services with accounts under their direct supervision. Those accounts created by guardians will fulfil specific and strengthened safety requirements, including having carried out and published an assessment of the impact of its service demonstrating the lack of risks for minors on its service. The proposed Regulation sets out how such video sharing platform services exceptionally accessible to children below 13 years through guardian-controlled access should provide a service that complies with safety by design requirements, is specifically designed for children and age-appropriate.

3.2.3. Provide harmonised safety by design obligations for digital services and systems accessible to minors

Following recommendation 3 of the Report of the Co-Chairs of the Special Panel, the proposed Regulation specifies, harmonises and extends safety by design rules for social networking services, video-sharing platforms services, online games, AI companions and general conversational chatbots accessible to minors. As noted by the Co-Chairs, extending and harmonising these rules ensure legal certainty and a high level of protection for minors across the digital environment ([258]). Overall, these rules address inherent risks that certain features and functionalities pose to children and aim at ensuring a safer environment by design and by default.

Safety by design requirements for all services and systems in scope include a clear prohibition on addictive design features as well as requirements to provide minors with options to tune and control information suggested by recommender systems. In addition, providers of online social networking services and of video-sharing platform services that use recommender systems are required to use specific metrics capturing quality, safety and mental-health outcomes to evaluate their recommender systems. Stricter guardrails are also established to lower the risk of minors encountering harmful content or getting stuck in so-called 'rabbit hole' effects in which minors

[256] *Ibid*, pp.52-60.
[257] In its Opinion 410309 of 8 January 2026, the Conseil d'Etat stated that parental consent derogations would ensure an appreciation of the child age and maturity and respect the role of parents in guiding their children and be associated to decisions that concern them in line with art.3(2), 4, 14(2) and 18(1) of the UNCRC.
[258] *Ibid*, p.109.

are exposed to prolonged chains of harmful content, including related to eating disorders, self-harm or suicide. Rules are set out to ensure that minors are provided with safe settings, including the disabling by default of the visibility of their profile to other users, of push notifications and geolocation, and provide minors with more control to manage these settings. To reduce risks of cyberbullying and grooming, contacts are limited with strangers and minors can easily block unwanted interactions. Additionally, requirements include prohibitions on spending maximisation, transparency and gambling techniques.

Online games must also implement safety by design obligations, prohibiting addictive designs that nudge children into continuing to play the game or returning to the game and requiring safe setting. Additionally, online games should implement safeguards to ensure that minors are not led to initiate contacts on other risky services.

Specifically, and in addition to these requirements, considering the risks posed by AI companions and general conversational chatbots and building on the DSA and the AI Act, such AI systems should fulfil additional obligations to ensure that AI companions and general conversational chatbots are safe for minors. In particular, providers of AI companions and general conversational chatbots are required to put in place strong child-safety protections, including designing systems so minors are not exposed to design features and systems behaviours that are likely to create emotional dependencies, and carrying out testing and post-market monitoring to identify and mitigate harms to minors' safety, health, fundamental rights and well-being (except for systems provided by a micro or small enterprise) . Where such systems are deployed as a functionality of an online social networking services, of a video-sharing platform services, of an online game, the providers of those services should ensure that AI companions and general conversational chatbots are not automatically activated, that minors have the possibility to opt out of their used, where enabled, and are not encouraged to use them.

Additionally, software application stores are required to put in place an age rating system to establish the age-appropriateness of applications disseminated through their service. The providers of such services should ensure that minors are prevented from purchasing or downloading an app that is inappropriate for their age. In addition, where the provider becomes aware of applications which primarily consist of content that is subject to a minimum age under applicable Union law or national law in compliance with Union law, they shall prevent minors from downloading or purchasing such an application below that minimum age. A code of conduct would help create common methodologies and criteria for such age rating systems, building upon current industry practice. Codes of conduct are also foreseen in regard to online networking services, video-sharing platforms, online games, as well as AI companions and general conversational chatbots.

Under the proposed Regulation, requirements to ensure the agency of children online are also established. In line with Recommendation 2 from Chapter 4 of the Report of the Co-Chairs of the Special Panel, the proposed Regulation also strengthens reporting mechanisms. Such tools must be effective, accessible and child friendly enabling minors to get rapid support and appropriate help upon notifying. Parents are also supported through the easy-to-use, interoperable and age-appropriate parental control tools, thereby implementing Recommendation 7 of Chapter 4. Such tools for example will be mandatory for providers of AI companions and general conversations chatbots, software application stores and online games for children below the age of 13 years. In other words, those providers will be required to ensure that access to their services and systems referred below the age of 13 years is only enabled and controlled by means of the tools for guardians. Rules are established to ensure such tools enable parents to report content on behalf of their child and to manage their account settings as well as

time-spent limits. To ensure these tools are effective, the proposed Regulation sets out a requirement for providers to encourage their uptake by parents. Those tools, as well as time limits, must respect children's evolving capacities and the right to privacy. They are complementary to other safety by design requirements, they should not replace any other measures to ensure the safety of children.

3.2.4. Establish clear requirements and criteria for the use of age assurance systems to underpin the access delay and the implementation of safety by design measures

The implementation of access delays and of safety by design rules requires robust and effective age assurance systems. In line with Recommendation 2 of Chapter 3 of the Report of the Co-Chairs of the Special Panel, the proposed Regulation establishes clear criteria and safeguards for the use and deployment of such systems, ensuring proportionality, data protection and non-discrimination.

The proposed Regulation requires age verification and age assurance for three reasons. First, the access delay requires age verification before account creation for certain social networking and video-sharing services. In this case, providers should exclusively on an EU Age Verification Solution using and EU proof of age attestation, in accordance with the EU Age Verification Scheme. Second, the safety by design obligations may require age assurance to enable settings and features reserved for adults. For instance, a platform may prompt adult users to prove that they are not a minor activate recommender systems drawing primarily on engagement-based signals, to get access to information that may pose a risk to minors when encountered repeatedly or to appear in the contact suggestions of other users. For the purpose of fulfilling the relevant safety by design obligations, providers may use alternative age assurance methods, such as age estimation, provided that they meet the requirements set out in the proposed Regulation. Providers of software application stores should use age assurance to prevent minors from accessing or purchasing age inappropriate or age restricted applications. Third, where an operating system has obtained an age signal in compliance with those requirements, it should, with the user's consent, enable the sharing of that signal with providers where required for compliance with the Regulation.

To remain proportionate, existing accounts can be exempted from the obligation to verify or assess the age, where the provider can determine with a high degree of confidence the account belongs to an adult or that the user is not a minor, as applicable. This avoids subjecting the entire adult population to unnecessary age checks. To further limit potential exclusion, providers must offer effective internal complaint-handling mechanisms that allow users to appeal incorrect age assessment.

To facilitate the implementation of privacy-preserving age verification solutions , Members States must ensure the availability of means for citizens to obtain a proof of age attestation and of at least an Age Verification Solution for the age thresholds set in the Regulation. Detailed technical, organisational, privacy and security requirements will be specified in limited secondary legislation.

Where parents create accounts for their minors or want to use tools for guardians, providers have to verify the parental responsibility of the respective adult over the child concerned. For providers to be able to carry out this verification, and for the parents concerned to be able to share this necessary proof, Member States must establish at least one privacy-preserving electronic means by which a guardian can obtain and present an attestation of parental

responsibility in respect of a minor. When doing so, Member States should ensure that such means are based on authentic sources established under national law, are free of charge for the guardian, and do not entail making information on parental responsibility accessible to providers or to the public beyond confirmation that parental responsibility exists. When providers already possess a signal that an adult is a guardian of a minor, the providers can rely on that as well. Additionally, adults should be able to self-declare that they are the parent and that they exercise parental responsibility. In those cases, providers should make reasonable efforts to verify that the adult is the guardian of the minor concerned. This verification should be carried out in a privacy-preserving manner and should not lead to additional processing of personal data that could enable the identification or tracking of the adult or minor concerned. The Commission may adopt a delegated act in order to specify the proof and signals that might indicate the parental responsibility.

3.2.5. Consolidate a coherent and robust enforcement framework to ensure timely and efficient implementation

To ensure efficient enforcement in line with Recommendation 5, no new enforcement structure is created to avoid conflicting and inconsistent enforcement. Rather, the enforcement of the proposed Regulation will benefit from the existing DSA and AI Act enforcement structures and procedures. The Commission remains responsible for the enforcement against VLOPs while Member States' Digital Services Coordinators are responsible for online platforms established on their territory. In relation to AI systems, the enforcement will rely on the AI Act framework and will be supervised by the AI Office within the Commission for AI companions [and general conversational chatbots] built on general-purpose AI models provided by the same provider or integrated into VLOPs or VLOSE in accordance with Article 75(1) AI Act. Member States' national market surveillance authorities designated under the AI Act will be responsible for other AI companions and chatbots. Non-platform online games will be supervised by the national authorities.

The proposed Regulation further establishes a new fast-track pathway for enforcement carried out by the Commission whereby a final decision can in principle be imposed in 90 days. Providers covered by the Regulation that have been designated as VLOPs are also required to submit a compliance plan to facilitate enforcement. The compliance plan must be audited by one or more independent auditors having proven expertise in the protection of minors online.. Finally, a coordination mechanism between the Commission and competent authorities is also established to cooperate on the assessment of incidents affecting the protection of minors across the Union and to rely on each other's expertise and resources.

3.2.6. Encourage and provide guidance to Member States on developing national measures and policies to support and complement the proposed Regulation.

As recognised by the Report of the Co-Chairs of the Special Panel, Regulation at Union level should be complemented and supported by action at national level, including through the proper prioritisation and allocation of resources to the protection of minors online ([259]).

The proposed Regulation thus imposes on Member States the obligation to support the objectives of the proposed Regulation with the establishment and implementation of national

[259] Fegert and Melchior, pp.132-134.

strategies to ensure that information and assistance in relation to the risks and harms addressed by the proposed Regulation are available and accessible to minors and their guardians. The proposed Regulation therefore imposes on Member States the obligation to develop and communicate strategies to fulfil the requirements of the proposed Regulation, and provides that Union funding should be made available to implement such strategies and the Commission should facilitate the exchange of best practices in particular related to digital literacy.

3.2.7. Recommendations of the Report of the Co-Chairs of the Special Panel

Chapter 3 of the Report of the Co-Chairs of the Special Panel analysed the existing legal framework and provided different recommendations to strengthen it and ensure a high level of protection for minors online. The following table provides an overview of how the different recommendations of the Report of the Co-Chairs of the Special Panel have been implemented in the proposed Regulation:

Recommendations of the Co-Chairs of the Special Panel	**New legislative instrument**
1/ Propose a **harmonised EU-wide access** restriction to social media and other digital services for minors under 13	Chapter II sets out a harmonised access delay for minors under the age of 15 for specific social networking services and video-sharing platforms. The age has been set to 15 considering the evolving capacities of the minors and the risks set out in the Report. Parents are provided with the possibility to set up guardian accounts in a safe environment for 13-15 reflecting the role of parents in guiding their children and better appreciating their individual circumstances.
2/ Introduce **effective age-assurance systems** to check age and underpin safety by design and age-appropriate approaches to protect and empower minors online	Chapter V provides clear rules for the implementation of age assurance to underpin both the access delay and safety by design requirements. It establishes clear criteria in terms of accuracy, reliability, security, robustness, non-intrusiveness, privacy, and non-discrimination. It further obliges Member States to ensure easy availability of trusted proof of age attestations, age verification solutions and attestation of parental responsibility.
3/ **Extend and harmonise rules on key safety features** in the design of social media and other digital services	Chapter III extends and harmonises rules on safety features for a wide range of digital services and systems accessible to minors, including online social networking and video-sharing services, AI companions, general conversational chatbots and online games. Those rules tackle addictive design,

	risks from recommender systems such as rabbit holes, unsolicited contact, safety and security of economic transactions protective default settings, child-friendly reporting and support tools, agency and tools for guardians..
4/ **Shift the burden of proof** to social media and other digital services providers to demonstrate that their products and services are safe for minors	Clear do's and don'ts shift the burden of proof to ensure that quick enforcement takes place on the basis of clear safety by design requirements providing for a legally binding standard on companies to design for children. Additionally, VLOPs are required to present to the Commission compliance plan shortly after entry into force of the Regulation. This compliance plan must be independently audited, and the Commission can request a corrective action plan in case of identified shortcomings. It should be noted that a broader ex ante assessment for every digital service accessible to children was considered. However, there are significant concerns from both a legal and practical perspective. Such an ex ante assessment would conflict with the freedom to provide information society services under Article 3 and the prohibition of prior authorisation under Article 4 of the E-Commerce Directive. In addition, considering the high number of digital services and systems on the market, a high number of requests to a single authority can lead to a system lacking credibility, and a lack or absence of meaningful decisions. The practical feasibility of such a system would depend on the availability of sufficient supervisory resources. Prior authorisation could also discourage the development and deployment of genuinely innovative safety measures because of the increased regulatory burden on digital services and systems, and incentivise providers to exclude minors from their services altogether.
5/ Strengthen **enforcement** and evaluation capacities	Chapter VII outlines the enforcement framework for this proposed Regulation. Building on the DSA and AI Act framework, it ensures consistency and coherency with the existing legal framework. It further provides for an expedited enforcement structure and a coordination systems for the assessments of

	incidents affecting the protection of minors, therefore strengthening enforcement.
7/ Member States can introduce **additional precautionary access** restrictions to social media and other digital services as of 13	The proposed Regulation does not provide for flexibility for Member States to introduce additional precautionary access restrictions. Taking a precautionary approach, the proposed Regulation sets a higher age for access delays at 15 years old. It provides however flexibility for parents to create accounts for children under 15, subject to their supervision and specific safety requirements. This enables parents to better consider their national contexts, but also the specific individual contexts and circumstances of their child. Additionally, this fully harmonised access restriction ensures legal certainty, lowers compliance costs and provides an equivalent level of protection for children across the European Union. The age of 15 also reflects many of the national proposals and discussions.
9/ Continuously **monitor and evaluate** the impact of measures implemented	Chapter IX of the proposed regulation sets out how the proposed Regulation will be reviewed, notably in terms of the effectiveness of the access delay, the personal scope of the access delay and the safety by design requirements, as well as the impact of the regulation on the right to freedom of expression and information. This review shall account for experience gained in the implementation of the proposed Regulation as well as technological, market and legal developments.

Chapter 4 of the Report of the Co-Chairs of the Special Panel further set out important recommendations to ensure the respect of children's rights and their autonomy. The following have been implemented in the proposed Regulation:

Recommendations of the Co-Chairs of the Special Panel	**New legislative instrument**
2/ Strengthen **complaint and reporting mechanism** and consumer rights for children and adolescents.	Section VI of Chapter III requires providers of digital services and systems in scope to provide easy to access and child friendly reporting systems. They must ensure that

	reports from minors and guardians are addressed as a priority.
7/ Ensure parents and carers are continuously supported by state-of-the-art and up-to-date **control and supervision tools.**	Article 20 further sets out that tools for guardians must be effective, accessible and user-friendly. They shall not disproportionately restrict minor's right to privacy and enable autonomy and agency in line with children's evolving capacities.
4/ Mainstream digital education and literacy actions for minors, parents and caregivers, teachers and educators; and 8/ Ensure sufficient public funding and common standards for civil society organisations and peer counselling	Chapter VI provides for Member States to develop national strategies to support the objectives of protecting children online, and access Union funds to implement such action.

3.3. A comprehensive regulatory framework for the protection of minors online

The proposed Regulation builds on the existing legislative framework for the protection of minors online and complements upcoming initiatives. By specifying and supplementing the DSA and the AI Act, it provides continuity and coherence to the EU regulatory framework for digital services and AI systems while developing an adapted legislative framework with specific requirements for the protection for minors online.

Upcoming initiatives will further reinforce the framework for the protection of minors online in the European Union. The ongoing evaluation and upcoming review of the AVMSD will specifically look at the protection of minors as viewers and will ensure that they are sufficiently protected when watching audiovisual content. Considering new threats and risks, it will examine whether further specification of the concept of harmful audiovisual content is needed, and what measures are necessary to ensure that minors do not encounter such content.

The Digital Fairness Act (DFA) further aims at strengthening the protection of minors online as consumers. Consumer law plays an important role in providing a safety net covering all types of traders interacting with children. It will continue to acknowledge minors as vulnerable consumers and protect them, in full complementarity with sector specific legislation, such as the proposed Regulation, from unfair and aggressive commercial practices.

Additionally, the proposal for a Regulation to prevent and combat child sexual abuse, once adopted, together with the recently adopted Recast of the Child Sexual abuse Directive, will strengthen the EU framework against child sexual abuse and exploitation, both online and offline. They will improve prevention, investigation and support for victims. As announced in the ProtectEU Strategy, the European Commission will an action plan on the protection of children against crime, which aims to complement existing instruments and fill gaps, notably strengthening coordination on the protection of children from crime both as victims and perpetrators, both online and offline.

Chapter 3 of the Report of the Co-Chairs of the Special Panel provided for some recommendations in relation to the overall regulatory framework. The table below explains how those recommendations will be implemented:

Recommendations of the Co-Chairs of the Special Panel	New legislative instrument
6/ Swiftly adopt measures to ensure social media and other digital services providers have **clear obligations to prevent, detect, report and block child sexual abuse** online, including interpersonal communication	Negotiations are ongoing on the Regulation to prevent and combat child sexual abuse. The recent changes in the AI Act introduced by the AI Omnibus prohibit AI systems generating child sexual abuse material, which will become applicable as of 2 December 2026.
8/ Strengthen **consumer protection policies** to protect minors online	Key protections for minors in the digital environment are embedded in this proposed Regulation. The upcoming Digital Fairness Act will complement this proposed Regulation with specific protection from a consumer law perspective,
10/ When processing children's data under the GDPR, social media and other digital services should ensure children's best interest are a primary consideration	The protection of minors remains a priority under the GDPR, as exemplified by the enforcement actions in the field. The EDPB adopted a "Statement on age assurance" in 2025 and, as stated in the EDPB strategy 2024-2027, it is currently working on guidelines on the processing of personal data of children.
11/Ensure effective implementation of the Product Liability Directive	The revised Directive entered into force on 8 December 2024 and must be transposed by Member States by 9 December 2026.

Non-legislative actions also complement this framework. The BIK+ Strategy supports the implementation of the EU's legislative instruments through awareness raising campaigns, capacity building, and direct engagement with children, parents and educators. The network of Safer Internet Centres (SICs), co-funded by the EU, reached more than 46 million Europeans in 2025. The SICs include an awareness centre, a helpline for children on online risks, and a hotline for anonymously reporting suspected child sexual abuse material. The BIK+ platform further offers a comprehensive collection of educational resources designed to support children's digital literacy, as well as parents, caregivers and educators.

Finally, child safety online is a global challenge requiring international cooperation. The proposal is consistent with the Union's external policies, including the International Digital Strategy (2025) through which the EU expands and deepens its cooperation bilaterally, regionally and multilaterally ([260]). The proposal harmonises legislation EU-wide which will support the effectiveness of the EU's external cooperation and global influence in child safety online.

[260] Joint Communication to the European Parliament and the Council An International Digital Strategy for the European Union (JOIN(2025) 140 final).

4. IMPACTS: A SAFER ONLINE ENVIRONMENT FOR CHILDREN

The impacts of the proposed Regulation have been evaluated, focusing on public health, fundamental rights and economic impacts. The evaluation builds on existing evidence, inter alia gathered in the context of the meetings of the Special Panel and the Report of the Co-Chairs of the Special Panel, the consultation process on the DSA guidelines on the protection of minors, the impact assessment of the DFA and of the AVMSD review. This was complemented by an additional study on the fundamental rights and economic impact of age assurance, as well as reference to several sources of evidence available, including relevant information shared by national authorities in the context of the European Board of Digital Services, or international partners such as the UK's Ofcom and Australia's eSafety Commissioner in the context of exchanges under existing agreements with these authorities.

To further complement the existing evidence, an additional study ('the external study') was procured by the Commission for the purpose of this Staff Working Document. The results of the study are expected to be published in Q4 2026. The study examined the impact of age assurance on the fundamental rights of children as well as adults and looked at the economic impacts of implementing age assurance solutions from the perspective of the services and systems in scope.

4.1. Public health

Overall assessment

The proposed Regulation is expected to improve minors' health and well-being through three main pathways. It would delay access for under-15s to a limited set of higher risk services, restrict design features and recommender practices associated with harmful or compulsive use, and require age assurance and other safeguards to support age-appropriate protections in practice. It is a targeted measure, as it applies only to selected services, systems and features that present risks to minors, while broader safety by design obligations are intended to make services and systems in scope accessible to minors safer by default. Benefits are expected to be greatest for groups that are more exposed or more vulnerable to online harms, including younger adolescents, girls, minors with pre-existing mental health difficulties, and more marginalised groups. The scale of the effects will depend on effective implementation, including robust age assurance, provider compliance with design obligation, and timely enforcement.

4.1.1. Direct health impacts

Evidence indicates that minors 'online experiences are associated with adverse mental health outcomes, in particular depression and anxiety, and that these effects can be stronger for minors who already face vulnerabilities. Given this evidence, the proposed Regulation is expected to have positive direct health effects by reducing exposure to harmful online conditions and by requiring providers to build in stronger protection for minors from the outset.

As outlined in Section 2.1, evidence points to a clear association between minors' online interactions and adverse mental health outcomes, particularly depression and anxiety, and

online experiences may also reinforce difficulties that are already present ([261],[262],[263],[264],[265]). Accordingly, the proposed Regulation focuses on reducing risk to minors' privacy, safety and security through safety by design obligations applicable to social networking services, video-sharing platform services, online games, AI companions or general conversational chatbots. Specifically, the proposed Regulation requires providers subject to the minimum age to put in place age verification methods to ensure that children cannot create accounts on their services and systems, and requires services and systems in scope to put in place safety by design measures to ensure a high level of protection for minors.

A first important element affecting the health of minors online concerns the timing of access to certain services and systems. Longitudinal evidence associates earlier access to smartphones and, with it, digital services, with a higher likelihood of mental health difficulties and insufficient sleep one year later, whereas access delayed until age 13 was not similarly associated with later depression ([266]). While this can be interpreted as an association rather than definitive proof of a causal age-specific effect, it does point to a meaningful role for the timing of access. In response, the proposed Regulation introduces a harmonised minimum age of 15 for holding an account on certain online social networks and video-sharing platforms. This is also intended as a precautionary measure to limit in particular exposure during early adolescence, when vulnerability to online harms appears to be elevated.

A second important element concerns compulsive or excessive use driven by the design of certain services or systems. Neurodevelopmental evidence indicates that adolescence, particularly between 13 and 15, is a period of heightened sensitivity to reward, peer feedback and external validation ([267],[268]), while impulse control and self-regulation are still developing ([269]). For this reason, the proposed Regulation is expected to benefit public health by limiting design choices that can encourage compulsive or excessive use among minors. It requires providers not to design, organise or operate services in a manner that is intended, or can reasonably be foreseen, to encourage compulsive or excessive use by minors. It specifically targets safety settings as well as design features such as autoplay and uninterrupted content consumption without effective and regular stopping points, notification, and features that incentivize repeated or more frequent engagement. By restricting such features as well as requiring effective time-management tools, the proposed Regulation is expected to reduce prolonged use, support self-regulation and lower associated negative impacts.

---

[261] Yang, C. C., Holden, S. M., Ariati, J., 'Social media and psychological well-being among youth: The multidimensional model of social media use', *Clinical child and family psychology review*, 24(3), 2021, pp.631-650.

[262] Vasconcellos, et al., 'Electronic screen use and children's socioemotional problems: A systematic review and meta-analysis of longitudinal studies', *Psychological Bulletin*, 151(5), 2025, pp.513–543.

[263] Schwartz, et al., 'Are social media use and popularity in the peer group linked during adolescence? A meta-analytic review', *Journal of Adolescence*, 97(3), 2025, pp.575-592;

[264] Madigan, S., et al., 'Association between screen time and children's performance on a developmental screening test', *JAMA pediatrics*, 173(3), 2019, pp.244-250.

[265] Teague et al.

[266] Bren, Z., et al., 'Smartphone Acquisition and Use at Age 13 Years and Health Outcomes at Age 14 Years', *JAMA pediatrics*, 180 (8), 2026, pp.858–866.

[267] Nesi, J., Telzer, E. H., Prinstein, M. J., 'Adolescent Development in the Digital Media Context', *Psychological Inquiry*, 31(3), 2020, pp.229–234.

[268] Orben, A., et al., 'Mechanisms linking social media use to adolescent mental health vulnerability', *Nature Reviews Psychology*, 3(6), 2024, pp.407–423.

[269] Orben, A., Przybylski, A. K., 'The association between adolescent well-being and digital technology use, *Nature Human Behaviour*, 3, 2019, pp.173–182.

A third important element concerns sleep, which is closely linked to minors' cognitive development, emotional regulation and mental health. Evidence show that screen use and online platform use can reduce sleep duration and quality through the displacement of sleep time, psychological stimulation before sleep and the suppression of melatonin ([270]). Evening screen use and prolonged engagement with online services and systems are associated with delayed sleep onset, reduced sleep duration and lower sleep quality, including through greater psychological stimulation before bedtime and suppression of melatonin production ([271],[272]). Poor sleep, in turn, negatively affects minors' attention, memory, emotional resilience, and daytime functioning, and is associated with impaired cognitive functioning and greater vulnerability to anxiety and depression ([273]). The proposed Regulation addresses these risks by requiring time-management tools and notification settings that may undermine minors' ability to disengage, especially during core sleeping hours, thereby mitigating an important mechanism through which online use may harm mental health.

The combined effect of these measures is expected to improve minors' mental health and well-being by delaying younger adolescents' access to higher-risk services, reducing exposure to addictive or excessive-use design features, and mitigating sleep-related harms through safer service design.

As for AI chatbots and AI companions, the safeguards foreseen in the proposed Regulation are expected to help protect minors' health, and in particular mental health, by making AI systems and their use safer, less manipulative, and less likely to encourage harmful use or excessive attachment. Safety by design requirements and safeguards on disabling by default the persistent conversational memory of interactions with minors should help preventing such AI systems from accumulating sensitive data of minors and potentially reinforce harmful interaction patterns over time. t. Limits on attachment-developing features could help prevent unhealthy emotional attachments and reduce the risk of children treating chatbots as trusted human companions. The same measures against addictive design and tools for effective time control are also envisaged for AI companions and chatbots so similar positive impacts on the health and wellbeing of minors are expected. Requiring providers of AI companions to carry out state-of-the-art evaluations and testing before release and regularly afterwards will help protect minors' health by early identification of health risks (e.g. testing can reveal whether a system encourages harmful behaviours, emotional dependency, or unsafe advice affecting physical or mental health), and safer system design from the outset. Testing at later stages and post-market monitoring is expected to contribute to ongoing protection as risks evolve or new risks or patterns of harm appear. This contributes to minors' health by underlining a preventive and continuous safety approach: risks to physical, mental, and emotional health can be identified earlier, mitigated more effectively, and monitored over time as minors interact with the system in practice.

[270] Vasconcellos, R. P., et al., 'Electronic screen use and children's socioemotional problems: A systematic review and meta-analysis of longitudinal studies', *Psychological Bulletin*, 151(5), 2025, pp.513–543.
[271] Hale, L., Guan, S., 'Screen time and sleep among school-aged children and adolescents: A systematic literature review', *Sleep Medicine Reviews*, 21, 2015, pp.50–58.
[272] Chang, A.M., et al., 'Evening use of light-emitting eReaders negatively affects sleep, circadian timing, and next-morning alertness', *PNAS*, 112(4), 2015, pp.1232–1237.
[273] Johri, K., et al., 'Effects of sleep deprivation on the mental health of adolescents: a systematic review', *Sleep Science and Practice*, 9(1), 2025.

4.1.2. Indirect health impacts

Beyond its direct effects on mental health, the proposed Regulation is also expected to improve well-being indirectly by reducing the displacement of activities that are essential for healthy development. Excessive or compulsive use of social media and other online services and systems is associated with lower levels of physical activity, more sedentary behaviour, less time spent outdoors, reduced in-person social interaction and shorter or poorer-quality sleep, partly because time spent online can crowd out activities that support physical, social and emotional development ([274],[275],[276]). By prohibiting design features that encourage uninterrupted or repeated use, such as autoplay, endless content consumption and engagement-driven notifications, and by requiring effective time-management tools, including protections for core sleeping hours and school time, the proposed Regulation is expected to help minors free up time for offline activities that are important for physical health, social development and broader well-being.

A second indirect pathway concerns cognitive development and attentional functioning. Because the prefrontal and related systems for self-regulation, attention and executive control are still developing during childhood and adolescence, minors are especially vulnerable to environments that fragment attention and encourage constant switching between tasks, screens or applications ([277],[278],[279],[280]). Research further shows that frequent smartphone or platform notifications can disrupt concentration and reduce task performance even when they are not actively opened or checked ([281],[282],[283]). The proposed Regulation thus seeks to mitigate these risks focusing on minors as a particularly vulnerable cohort, by restricting design features that incentivize compulsive switching or prolonged engagement ([284]), and by requiring recommender systems not to exploit minors' vulnerability or attention. Specifically, recommender systems must not give primary weight to explicit engagement-based preferences when suggesting information, and minors must be given simple tools to control, modify or reset recommendations. The safety by design measures in the proposed Regulation are expected to

[274] Muppalla, S. K., et al., 'Effects of Excessive Screen Time on Child Development: An Updated Review and Strategies for Management', *Cureus*, 15(6), 2023.
[275] Calvert, S. L., 'Parasocial relationships with media characters: Imaginary companions for young children's social and cognitive development. In Cognitive development in digital contexts', *Academic Press,* 2017, pp.93-117.
[276] Marshall, S. J., et al., 'Relationships between media use, body fatness and physical activity in children and youth: a meta-analysis', *International Journal of Obesity*, 28(10), 2004, pp.1238-1246.
[277] Muppalla, S. K., et al., 'Effects of Excessive Screen Time on Child Development: An Updated Review and Strategies for Management', *Cureus*, 15(6), 2023.
[278] Baumgartner, S. E., et al., 'The relationship between media multitasking and executive function in early adolescents', *The Journal of early adolescence*, *34*(8), 2014, pp.1120-1144.
[279] Ji, X., Cui, N., Liu, J., 'Beyond screen time: commentary on early screen media multitasking as a developmental risk for executive function in preschoolers', *Pediatric Research*, 99(1), 2026, pp.12-13.
[280] Naik, V. S., et al., 'Impact of social media on cognitive development of children and young adults: A systematic review', *BMC pediatrics*, 25(1),2025, p.826.
[281] Kushlev, K., Proulx, J. D. E., Dunn, E. W., ""Silence your phones": Smartphone notifications increase inattention and hyperactivity symptoms", In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, *ACM Press*, 2016, pp.1011–1020,
[282] Stothart, C., Mitchum, A., Yehnert, C., 'The attentional cost of receiving a cell phone notification', *Journal of Experimental Psychology: Human Perception and Performance*, 41(4), 2015, pp.893–897.
[283] Fournier, H., et al., 'Attention hijacked: How social media notifications disrupt cognitive processing', *Computers in Human Behavior*, 108926, 2026.
[284] For example, services should not keep videos or posts playing without proper stopping points, send unnecessary notifications to pull children back, or use rewards and pressure to make them log in more often.

reduce cognitive overload and support better focus, which is closely linked to learning, emotional regulation, and healthy development more broadly.

At the same time, the proposed Regulation seeks to preserve beneficial online experiences while reducing the extent to which digital services systematically displace healthier offline activities. Its approach is to make providers responsible for designing services and systems that do not take advantage of minors' developmental vulnerabilities, rather than placing the full burden on minors or parents to manage harmful design on their own. In that sense, the expected indirect health benefits stem not only from reducing overuse, but also from creating digital environments in which healthy routines, attention management, and balanced online-offline habits are easier to maintain.

Overall, the proposed Regulation's indirect health benefits are expected to arise from four main effects: reducing the displacement of minors' physical activity, face-to-face interaction and sleep; and protecting minors' attention and cognitive development from constant interruptions and fragmented use;

4.1.3. Distributional effects

The health impacts described above are expected to have stronger protective effects for groups facing disproportionate online risks and, therefore, help to narrow existing inequalities. First, adolescents aged 13 to 15 and girls appear to experience more pronounced and persistent effects on depression and anxiety, consistent with evidence that this may be a period of heightened developmental sensitivity ([285],[286]). Minors with pre-existing mental health difficulties also require particular attention, as online experiences may reinforce existing vulnerabilities rather than only cause new harms ([287],[288],[289]).

Second, adolescents from disadvantaged socio-economic backgrounds are more likely to report harmful online experiences, including cyberbullying and problematic social media use ([290],[291],[292]). Although some young people from disadvantaged backgrounds may have fewer opportunities to replace online time with activities such as sports, clubs, or safe outdoor leisure, the evidence suggests they are also more exposed to the harms the proposed Regulation addresses. A similar pattern can be observed among LGBTIQ+ adolescents and minorities or marginalised groups. Safe online spaces may offer valued sources of peer support and connection, sometimes perceived as safer than offline environments ([293]). At the same time,

[285] Orben, A., et al., 'Mechanisms linking social media use to adolescent mental health vulnerability', *Nature Reviews Psychology*, 2024, 3(6), pp.407–423.
[286] Vasconcellos, R. P., et al., 'Electronic screen use and children's socioemotional problems: A systematic review and meta-analysis of longitudinal studies', *Psychological Bulletin*, 151(5), 2025, pp.513–543.
[287] Bertoni, E., Centeno, C., Cachia, R., Social media usage and adolescents' mental health in the EU. European Commission, Joint Research Centre (JRC), 2025.
[288] Beullens, K. et al.
[289] Vidal, C., et al.,'Social media use and depression in adolescents: A scoping review', *International Review of Psychiatry*, 32(3), 2020, pp.235-253
[290] Ronis, S., Slaunwhite, A., 'Gender and Geographic Predictors of Cyberbullying Victimization, Perpetration, and Coping Modalities Among Youth', *Canadian Journal of Psychology*, 34(1), 2017.
[291] Koch, T., Laaber, F., Florack, A., 'Socioeconomic status and young people's digital maturity: The role of parental mediation', *Computers in Human Behaviour*, 2024.
[292] Lu; World Happiness Report 2026; Prkno, D. et al.
[293] 5Rights Foundation, *Why digital platforms must be designed with LGBTQ children in mind*, 2020. [5Rights Foundation]

these groups face higher exposure to online hate and harassment ([294],[295],[296],[297]). Exposure to online hate speech has itself been linked to negative health outcomes, including panic and stress reactions, difficulty concentrating, and depression ([298]). Reducing exposure to such conducts or content is therefore likely to bring higher benefits to those most frequently targeted, including minors targeted based on ethnic or religious background, sexual orientation or disabilities, who report higher exposure to online hate speech ([299], [300]).

This means that whilst in principle minors from these backgrounds or groups might face some additional difficulties in adapting to a new situation in cases where they are not allowed to have accounts on certain services or systems anymore, overall they are also more likely to benefit more from stronger protections on services and systems that they and their peers use. Broadly, the proposed Regulation is thus expected to have stronger protective effects for such groups facing disproportionate online risks. By reducing exposure to harmful content and harmful online experiences, while preserving access to support information and connection, it may help narrow existing inequalities in mental and emotional health.

4.1.4. Risks and unintended effects

The proposed Regulation is designed to strengthen minors' online safety but its benefits are likely to emerge gradually and may be accompanied by unintended effects that should be acknowledged are mitigated.

First, the full positive impacts are likely to occur progressively rather than instantaneously. Experience from jurisdictions that have introduced broad age-based restrictions on social media is instructive in this respect. Australia introduced a nationwide minimum age of 16 for social media accounts in December 2025. Early evidence suggests that a substantial proportion of minors subject to the ban have nevertheless remained on social media, underlining the practical difficulty of enforcing age verification at scale particularly during the initial implementation phase ([301]). Research on the Australian experience also notes that any meaningful shift in social norms likely takes time ([302]). Under the proposed Regulation for the EU, however, even where minors circumvent age-based access restrictions, the core child-protection obligations would continue to apply to services accessible to minors. Providers would remain required to ensure a high level or privacy, safety and security for minors, would be prohibited from encouraging them to reduce those protections, and would need to ensure that safeguards are not easily circumvented through the design or operation of the service or system.

A second risk is displacement towards services or systems that may fall outside the minimum-age rule. If access is restricted on certain services or systems, minors may migrate towards

[294] eSafety Commissioner, *How common are experiences of seeing online hate among children in Australia*, 2025.
[295] 5Rights Foundation.
[296] Fundamental Rights Agency, *LGBTIQ equality at a crossroads: Progress and challenges*, 2024, p.72.
[297] Impact Assessment CSAR, p.17: Vulnerable children are at higher risk of online CSA. Recent survey data on childhood experiences show that online sexual harm was reported by 59% of transgender and non-binary respondents, compared with 47% of cisgender respondents; 65% of LGBQ+ respondents, compared with 46% of non-LGBQ+ respondents; and 57% of disabled respondents, compared with 48% of non-disabled respondents.
[298] Département fédéral de l'environnement, des transports, de l'énergie et de la communication (Suisse), *Avant-projet de loi fédérale sur les plateformes de communication et les moteurs de recherche (AP-LPCom): Rapport explicatif en vue de l'ouverture de la procédure de consultation*, Octobre 2025.
[299] Council of Europe, *Hate speech levels across Europe alarming, stronger action needed*, 2026.
[300] eSafety Commissioner 2023.
[301] Bursztyn et al.
[302] eSafety Early Insights 2026.

services or systems that are not covered by the minimum-age rule, potentially exposing them to environments with fewer safeguards. This risk is partly mitigated by the horizontal structure of the proposed Regulation, which extends safety by design obligations across online services and AI companion and general conversational chatbots that are accessible to minors. Those obligations apply irrespective of the size of the service and therefore help ensure that alternative services and systems also become safer by default.

Another issue that merits careful consideration is that some minors currently rely on online services and systems, including social media and chatbots, for support, information and connection. For some children and adolescents, online environments can provide access to mental-health information, peer communities, or crisis-related support that may feel more accessible than offline alternatives. Digital spaces may also create opportunities for self-expression, social connection and advice on where to seek help. At the same time, those same environments can expose minors to additional vulnerabilities. They may encourage the formation of new relationships in ways that increase exposure to harm, while certain online behaviours, such as curating an unrealistically idealised self-image, may intensify loneliness or social isolation ([303],[304]).

It is therefore important to distinguish between two separate issues. The first concerns access to support. The proposed Regulation requires providers to make it easier for children and adolescents to obtain help and to find reliable information when they encounter harmful or illegal content online. This includes directing them towards support services and trusted organisations at national and Union level. It also requires, where reasonable, clear warning messages in situations where minors are likely to publish or encounter content or interactions that may put their privacy, safety or security at risk. In practical terms, this means that support pathways related to their online experience on services or systems that they can access should remain available through provider-based tools and channels required under the proposed Regulation. This approach is consistent with broader EU action on youth mental health, including the Commission's Communication on a comprehensive approach to mental health ([305]) and the Better Internet for Kids strategy ([306]).

The second issue concerns participation in online social environments more generally. Evidence suggests that not all forms of online engagement affect minors in the same way. More active forms of use, such as posting, commenting or interacting with others, are often associated with greater well-being and stronger perceived social support, whereas more passive behaviours, such as browsing or scrolling without interaction, are more consistently linked to depressive symptoms, loneliness and stress ([307],[308]).

Overall, the proposed Regulation seeks to reduce minors' exposure to harmful or age-inappropriate online experiences while preserving the benefits that digital services can offer, including access to information, social connection and support. It combines age-based restrictions for certain types of services and systems with safety by design obligations for all

[303] Sala et al.

[304] Cataldo, I., et al ., 'Social Media Usage and Development of Psychiatric Disorders in Childhood and Adolescence: A Review', *Frontiers in Psychiatry*, 11, 2021. [Cataldo et al.]

[305] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a comprehensive approach to mental health (COM(2023) 298 final).

[306] BIK+.

[307] Cataldo et al.

[308] Bottaro, R., Faraci, P., 'The use of social networking sites and its impact on adolescents' emotional well-being: A scoping review', *Current Addiction Reports*, 9, 2022, pp.518–539.

services and systems in scope, including support tools, as well as the possibility for minors under the minimum age to access under certain conditions those services and systems that are safer and more appropriate for younger users. As children's online practices and the digital ecosystem will continue to evolve, the long-term effectiveness of the rules will also depend on regular review, evaluation and adaptation, so that the framework remains both proportionate and responsive to emerging technologies and developments. For that reason, the framework includes delegated and implementing powers, annual provider evaluation duties, and a future review clause requiring the Commission to assess, among other things, the effectiveness of delayed access and the broader scope of the obligations as technology and children's digital practices evolve.

4.1.5. Mitigations

The proposed Regulation addresses the risk identified above through a combination of delayed access for minors, harmonised safety by design requirements, and measures to monitor, test and evaluate the effectiveness of the measures. The mitigation logic of the proposed Regulation is cumulative. Delayed access seeks to prevent younger children from entering online environments considered higher risk before they are better able to cope with their design and interaction features. In parallel, safety by design obligations seek to reduce risks for minors who do access services, by requiring providers to make those services safer by default, less manipulative in design, and more responsive to children's privacy, safety and security needs. Age assurance supports both objectives, while annual monitoring, testing and evaluation are intended to ensure that safeguards remain effective over time. **Table 2A** provides a concise overview of the principal risks directly targeted by the proposed Regulation and the main mitigating provisions. **Table 2B** then identifies key limitations that could reduce the effectiveness of the proposed Regulation in practice and explains how the draft Regulation seeks to address them, while acknowledging residual constraints.

***Table 2A**: Risks the proposed Regulation directly addresses*

Risk area	How the risk manifest	Who/What is exposed	Relevant provisions in the proposed Regulation	Expected protective effect
Compulsive or excessive use	Addictive design features or commercial practices that make it hard for children to stop scrolling, watching or playing or spending money.	Minors using online services in scope or AI companions and general conversational chatbots.	Prohibition of addictive design; measures on safety of economic transactions; mandatory time-management tool.	Reduced compulsive use and stronger control, including over spending.

Unsafe recommender systems	Profiling- or engagement-based recommendations may exploit vulnerabilities and increase repeated exposure to harmful or risky content.	Minors exposed to suggested content.	Limits on profiling-based optimisation; obligations on recommender design; user-control and reset tools.	Safer suggestions; less manipulation; greater choice and control over content.
Unsafe default settings	Geolocation, microphone/camera access, account discovery, contact synchronisation or push notifications expose minors to risks from the outset.	Minors using online services in scope or AI companions and general conversational chatbots.	High privacy, safety and security settings by default, including turning off high-risk features.	Higher baseline protection from the outset.
Unsafe contact and interaction	Contact by unknown users, unwanted group addition, visibility of minors' interactions	Minors interacting with other users	Contact and interaction safeguards	Reduced unwanted contact and stronger control over interactions
Exposure to harmful content	Repeated exposure to harmful information or risky publishing/interactions	Minors across covered services	Recommender safeguards; support tools; warning messages;	Reduced exposure and better-informed choices
Early access to risky services	Children under 15 may register for services with high-risk features	Children below 15 seeking registration to high-risk services	Delayed-access rule; age verification; checks on existing accounts	Fewer younger children on high-risk services and delayed access to riskier online spaces.

Emotional dependencies on AI companions and chatbots	Features displaying behaviours or simulating emotions or interpersonal relationships in AI companions and general conversational chatbots lead minors to emotional dependencies on these systems	Minors using AI companions and [and general conversational chatbots]	Restriction of features likely to create emotional dependencies	Reduced emotional attachment to interacting AI systems

Table 2B: *Potential Limitation to the Proposed Regulation's Effectiveness and Corresponding Mitigation Measures*

Effectiveness risk	**Why it matters for outcomes**	**Affected measure(s)**	**Mitigation in proposed Regulation**	**Remaining limitation**
Circumvention of age checks/	Delayed-access protections are weakened if children bypass restrictions.	Delayed-access rules; age verification requirements	Mandatory age verification before account creation for services and systems subject to minimum age; self-declaration not sufficient; Member States must ensure availability of proof-of-age and at least one age verification solution	Technical and practical circumvention remains possible
Weak uptake or ineffective use of user tools	Safety tools only protect children if they are well designed, time management and reporting tools only if they are understandable, easy to activate and used in practice by children guardians	Time-management tools, recommender controls, safe setting, reporting tools, tools for minors, and guardian tools	Tools to be effective, accessible and user-friendly; minors must receive understandable information; settings must default to a high level of privacy, safety and security	Some tools may still be underused if perceived as burdensome or poorly understood.

Fragmented implementation	Uneven enforcement or infrastructure across Member States may create disparities in protection.	Age verification infrastructure; national competent authorities	Harmonised rules; DSA-and AI Act-based supervision and enforcement structure; Member State obligations on age verification availability	Day-to-day supervision and national enforcement practice may still vary.
Ecosystem dependencies	Protections depend on cooperation between app stores, operating systems and service providers.	Reuse of age signals; app store and operating system duties; interoperability of guardian tools	App stores and operating systems must enable reuse of age signals; very large platforms must ensure interoperability of guardian tools with third-party tools	Effectiveness still depends on technical compatibility and provider cooperation.

The proposed Regulation includes delegated and implementing powers, annual provider evaluation duties, and a future review clause requiring the Commission to assess, among other things, the effectiveness of delayed access and the broader scope of the obligations as technology and children's digital practices evolve.

Overall, the proposed Regulation combines prevention, safer service design and accountability in a structured and proportionate manner. Table 2A and 2B show, first, the direct linkage between the main risks and the corresponding protective measures and, second, the principal implementation challenges and the mechanisms to mitigate them. Together, they demonstrate how the framework is intended to reduce current harms but also to remain adaptable as risks and technologies develop.

4.2. Fundamental Rights

Article 3(3) of the TEU establishes the objective for the Union to promote the protection of the rights of the child. This fundamental right is among the values on which the Union is founded pursuant Article 2 TEU. One of the core objectives of the proposed Regulation is to ensure a high level of protection for children online, the respect, protection and fulfilment of children's rights are therefore central to the proposed Regulation. As the online environment is marked by the complexity of interests at stake and the need to maintain a fair balance in mitigating risks for children's rights as well as for the fundamental rights of all users, additional fundamental rights considerations have been duly taken into account. The impact of the proposed Regulation on fundamental rights besides the impact on children's rights is considered with a focus on the impact of age assurance requirements, as these measures would be potentially affecting all

users, whereas the minimum age and safety by design requirements will directly and primarily affect minors. In line with this approach, the impact on the fundamental rights that are broadly considered by experts and civil society ([309],[310],[311],[312],[313]) to be most at risk of being affected for users subject to age assurance have been considered in more detail.

4.2.1. Rights of the child (Art 24 of the Charter of Fundamental Rights)

Overall, the proposed Regulation aims at improving the respect of the rights of the child online ([314]). In line with their best interest, the access delay aims at ensuring a better protection of the health and security of minors' online ([315],[316]). The minimum age does not curtail their access to the digital environment as a whole but rather set a delayed start date for their autonomous access to a set of digital services that are deemed to be risky or harmful to the privacy, safety and wellbeing of younger minors. The delay particularly takes into account the evolving capacities of children, and as explained in the Report of the Co-Chairs of the Special Panel, it considers the importance for children under 15 to gradually transition to autonomous use, whilst also ensuring that such autonomous use above 15 years old remains safe by design. Indeed, the proposed Regulation sets out that in cases where a service is specifically designed for children and provides limited functionalities and all the appropriate safeguards to pose no risks for children under the minimum age, such services may be accessible under parental supervision. Additionally, exceptions to the delay are provided to ensure that the set of services covered by the minimum age does not cover those where children may need access to information, education materials, public services or other activities that are in their best interest.

Access restrictions for minors could indeed be considered as an interference with other rights of the child, notably the right to freedom of expression, participation and access to information, and they must therefore pursue a legitimate aim and be proportionate for such objective. As recognises by several judicial instances, limitations to freedom of expression and other rights should thus be justified in the best interest of the child. This should serve as principle to balance the different rights of the child in view of the recognised and documented risks to the safety, wellbeing, free development and self-determination of minors stemming from the use of types of services and systems that present certain features – i.e., notably the online environments created by "social media+", which according to the Report of the Co-Chairs of the Special Panel "expose them to diverse risks for their physical and mental health and development at different ages" ([317]).

---

[309] Shaffique and van der Hof.
[310] Beltrán, M., de Salvador, L, 'Implications of Age Assurance on Privacy and Data Protection: A Systematic Threat Model', in *Privacy Technologies and Policy,* Jensen, M., Lauradoux, C., Rannenberg, K., Eds.; Springer Nature Switzerland: Cham, 2024; pp 1–22.
[311] Shaffique, M. R., van der Hof, S, 'Behavioural Profiling for Age Assurance: Do the Ends Justify the Means?', *International Data Privacy Law*, 2025.
[312] Livingstone, S., et al., 'Children's Rights and Online Age Assurance Systems: The Way Forward', *The International Journal of Children's Rights*, 32 (3), 2024, pp.721–747.
[313] Niestadt, M., *Debate on Setting a Minimum Age for Social Media*, European Parliamentary Research Service, 2026.
[314] As enshrined in the United Convention on the Rights of the Child adopted in 1989, which has been ratified by all Member States and on which Article 24 of the EU Charter of Fundamental Rights is based.
[315] Conseil d'Etat, Opinion 410309 of 8 January 2026, §23.
[316] OECD, *Recommendation of the Council on Children in the Digital Environment*, OECD/LEGAL/0389.
[317] Fegert and Melchior, p.10.

The Report of the Co-Chairs of the Special Panel explains how the different phases in the years from 0 to 15 are particularly important for minors' cognitive, emotional and social development, as well as for the evolution of their personality, identity and value systems. Risks evolve with the development of the child. From risks as passive online users in early ages, when much needed care risks to become neglected if substituted by screentime, thus affecting children's attention span, language acquisition, and socio-emotional development; through risks of mismatch between continuous exposure to external stimulation and children's evolving capacities and emerging self-perception in the years leading to adolescence; to risks of convergence of developmental sensitivities and platform-driven amplification of content and interactions in early adolescence. Research shows mental health impacts and that children are especially vulnerable under the age of 13, and until 15 adolescents transition into autonomy, so whilst supervision by caregivers and educators gradually becomes ineffective, risks are increasingly shaped by social elements of digital services, rather than individual behaviours, thus adolescents from 13 to 15 are at the peak of vulnerability to mental health issues. It is thus important to ensure that children's rights to safety as well as healthy development and self-determination are enjoyed in conjunction with other rights – notably to information, expression or participation, free from the substantial impacts that certain online services can have on them.

Furthermore, as also enshrined in Article 24(3) of the Charter and recognised in the Report of the Co-Chairs of the Special Panel, it is important to take into account the role of guardians in supporting the minor's transition to autonomous and safe use of digital services. Until the age of 15, adolescents gradually transition from supervised development to guided online use and evolving autonomy. They increasingly encounter opportunities presented by the online world to connect, learn and develop and share their interests with others, thus whilst they may not benefit from being fully limited in their exposure, they can still enjoy safeguards and be protected from potential harm during these stages of developmental vulnerability, characterised by the convergence of identity formation, heightened socio-emotional sensitivity and decreasing effectiveness and importance of supervision by caregivers and educators. The proposed Regulation thus set out that guardians should be able to support children with the creation of child-friendly accounts, subject to safeguards ensuring effective parental supervision on the service, including the ability to adapt account settings progressively to the minor's evolving capacities, limit the duration of access and suspend the account if necessary.

The delayed start date in the proposed Regulation is therefore proportionate to the risks posed by the types of services and systems in scope, which by design present characteristics, features and functionalities that expose minors to risks related to inappropriate content, contacts, conducts and commercial practices. However, besides the services and systems subject to the general exception mentioned above, there exist the risks that some services may fall in scope of the age restriction without an established and demonstrated risk to the safety of minors, for instance designed and operated specifically and in the best interest of minors. This risk may be considered in view of a precautionary principle, which as explained in the Report of the Co-Chairs of the Special Panel also means that "age restrictions may be a necessary precautionary step until social media+ spaces are shown to be safe […] or until safe alternatives emerge" and represent "immediate measures to achieve the long-term goal of ensuring social media+ spaces are safe" ([318]). The proposed Regulation thus foresees that children can access under parental supervision services that can be deemed to be designed and operated in the best interest of children. This provides the margin for guardians to take into account the specific circumstances

[318] Fegert and Melchior, pp.6-7. See also Lievens, E., 'Growing Up with Digital Technologies: How the Precautionary Principle Might Contribute to Addressing Potential Serious Harm to Children's Rights', *Nordic Journal of Human Rights*, *39*(2), 2021, pp.128–145.

of the child, including maturity, personal situation and socioeconomic context in connection to the type and nature of the service and system, and therefore mitigate the risk of an excessive and disproportionate age restriction, in the best interest of the child, including by adapting the settings and safeguards of the services to the age and needs of the minor.

Safety by design requirements are also key to ensure the rights of the child online ([319]), including for those minors above the minimum age that increasingly experience the online environment in autonomy. Providing a safer environment for minors aim at ensuring that everyone can participate and enjoy the opportunities of the digital world without risk of being exposed to risks for mental wellbeing, harmful content or behaviours and other forms of online abuse or commercial exploitation. Thus, safety by design requirements on safe settings provide protection from exposure of minors and their content or information to unwanted contacts, abusive behaviours by other users, or risks of developing compulsive or addictive behaviours or mental health conditions linked to exposure to harmful content. Obligations on recommender systems further aim at ensuring the quality, diversity and age appropriateness of information suggested to children ([320],[321]). This is critical to stimulate children's right to developing and holding their own opinion ([322]). Furthermore, the proposed Regulation provides that effective, visible and child-friendly mechanisms for reporting and support should be available and accessible for minors to report content, accounts, groups, features and behaviour that may negatively affect their privacy, safety and security when using the service, as well as to be informed and supported in understanding risks prior to engaging in certain activities such as posting or sharing content or enhancing the visibility of their information or that of other users.

To ensure the protection of minors online, robust and effective age assurance systems are recognised as necessary to recognise their presence online and limit their exposure to illegal or harmful products or services, as well as a being a precondition for an age-appropriate, safer and more empowering environment for children ([323]). With its clear requirements, the proposed Regulation will ensure that age assurance systems are effective, not easily circumventable, respectful of children's privacy and implemented in line with their best interest. In recognition of the key role that parents play in the upbringing and development of their children, the proposed Regulation mandates tools for guardians, which should be available and apply as appropriate for all services and systems and all minors, in addition to supervised accounts for under 13, and accounts created by guardians for 13-15. Those tools must be provided in line with the evolving capacities of children, and in respect with their rights to privacy.

As for additional requirements for AI companions and general conversational chatbots, the proposed Regulation supports the child's rights, including their dignity, mental well-being and best interests. The proposed Regulation requires providers to avoid design features and system behaviours that simulate interpersonal relations that are likely to create emotional dependencies. This can help protect children from becoming emotionally attached to a chatbot in ways that may affect their social development, autonomy or emotional balance. Safeguards on addictive designs, safe settings and safe and secure economic transactions are also set out. Performing state of the art evaluations and testing before and after the AI companions are placed

[319] Committee on the Rights of the Child, *General comment No.25 (2021) on children's rights in relation to the digital environment*, 2 March 2021, §70, 77, 78 and 116. [UNGC 25]
[320] *Ibid,* §50-54.
[321] European Court of Human Rights, Case of Handyside v. The United Kingdom, No. 5493/72, 1976: the case recognised the right for children to receive information appropriate for a child's age and maturity.
[322] UNGC 25, §61.
[323] UNGC 25, §114.

on the market and post-market monitoring strengthen the practical protection of minors' fundamental rights over time promoting a safer digital environment.

4.2.2. Private life and privacy of communication (Art 7 of the Charter) and personal data protection (Art 8 of the Charter)

The proposed Regulation should not prejudice the high standard of personal data protection and protection of privacy of communications and private life set in EU legislation. Furthermore, measures aimed at ensuring children' online safety can be expected to enhance their privacy. Several safety by design measures aim at ensuring that their information remains private or only shared with a limited circle if the minor so decides.

The obligation to establish age assurance systems to support the implementation of the access delay and the safety by design measures imply the processing of personal data. Considering the need for a consistent approach and the existing obligations in terms of age assurance present in EU and national legislation ([324]), the European Data Protection Board (EDPB) provided specific guidance and high-level principles outlining key considerations for age assurance systems to be in line with data protection requirements ([325]).

The proposed Regulation establishes clear requirements for the deployment and use of age assurance systems in line with the principles outlined by the EDPB ensuring a high standard of data protection. These criteria include a high level of accuracy, reliability, robustness, security, non-discrimination and non-intrusiveness. Following a risk-based approach and ensuring proportionality, age verification is only mandated for the implementation of the access delay.

As noted in the external study, age verification – whether through the EU Age Verification Solution or through comparative solutions – can be implemented in ways that are privacy-preserving by design. In that context, the external study recommended that to mitigate rights interferences, the legislative instrument should require services to use age verification methods that utilise double-blind architecture, and which incorporate technological innovations like zero-knowledge proof cryptography. The proposed Regulation requires, where age verification is required, to rely on the EU Age Verification solutions, which will have to meet the highest standards in terms of privacy and data protection, using zero-knowledge proof cryptography.

Moreover, as noted in the external study, many privacy and data protection risks that arise in the context of age assurance relate to how age assurance is *deployed* by service providers and how age assurance systems are *operated*. This includes questions of what personal data is collected, how it is processed, which entities it is shared with, and how it is stored. The study further noted that these risks can be largely mitigated through adherence to the General Data Protection Regulation, and through clear application to age assurance providers of the GDPR's provisions on data minimisation, purpose limitation, transparency, and data protection by design and default. The proposed Regulation ensures this, by laying down additional safeguards for age assurance providers and the providers of services relying on age assurance solutions, such as further specifying the application of principles of purpose limitation, data minimisation, and data protection by design and by default. Furthermore, it should also be underscored that service providers' implementation of the proposed Regulation's age assurance requirements are

[324] For an overview of EU legislation and examples of national legislation see Galissaire, J., *Mind the Gap: Age assurance and the limits of enforcement under EU law*, 13 October 2025.
[325] European Data Protection Board, *Statement 1/2025 on Age Assurance*, 11 February 2025.

subject to the horizontal rules of the GDPR, and they must be undertaken in strict accordance with GDPR's principles on data processing.

Separately, the external study characterised the age assurance market as a vibrant and mature one, where age assurance providers are increasing competing and innovating on privacy and accessibility grounds. The study recommended that any future legislative proposal capitalise on this reality, by allowing service providers in scope of an age assurance requirement to utilise third-party age assurance solutions that meet high standards of privacy and security. By enabling third-party age verification solutions to adopt the EU Age Verification blueprint and by allowing service providers to adopt a range of age assurance methods for the purposes of safety by design, the proposed Regulation leverages the competitive forces of the market in favour of privacy-preserving approaches.

Accounts created by parents for their children also further requires verifying that the adult is the guardian of the minor concerned. The proposed Regulation establishes that such verification must be done in a privacy-preserving manner, through the use of 'zero knowledge proof', and not lead to the additional processing of data that could enable the identification or tracking of the adult or minor concerned.

Ultimately, by enshrining safeguards in law, affirming the applicability of the GDPR, and setting a baseline standard for how third-party age assurance solutions should operate, the proposed Regulation provides for the effective use and deployment of age assurance systems while ensuring a high standard of data protection for their use. The proposed Regulation provides for clear legal standards, which will promote the deployment of an innovative market of age assurance solutions respectful of fundamental rights.

As for AI companions and general conversational chatbots, the requirement for providers to avoid features posing risk of emotional dependencies protects minors' private life because systems that simulate human emotions or relationships can encourage children to disclose intimate thoughts, feelings, routines, fears, or family matters as if they were speaking to a trusted person or friend. Limiting such design features therefore helps safeguard minors against both undue emotional influence and against the extraction or exposure of intimate aspects of their private life.

4.2.3. Freedom of expression and information (Art 11 of the Charter)

The proposed Regulation does not provide for a prior authorisation scheme. Such measures can amount to a severe limitation to freedom of speech. Additionally, the proposed Regulation does not remove the right of an individual to remain anonymous online, which could have a chilling effect on freedom of expression. The obligations set out in the proposed Regulation in terms of age assurance are not an obligation of identity verification and clear safeguards are established to this effect in the proposed Regulation. Age assurance solutions shall only share an anonymised yes/no answer to the age question.

As noted in the external study, providing end users with a choice of age assurance methods and/or deployment models as well as fallback options (e.g. manual enrolment) can mitigate the chilling effects of the age assurance process on freedom of expression. It would respond directly to the situation where users opt-out of assuring their age owing to concerns about *specific* age assurance approaches (rather than the principle of age assurance itself) or because they lack the necessary pre-requisite technology/identity artifacts. The proposed Regulation accounts for this potential interference with freedom of expression, by enabling the use of third-party age

verification solutions that conform to the high standards of privacy and security that are set by the EU Age Verification Solution, and in the case of the safety by design requirements, by allowing for a choice of different *methods* of assurance.

The study further noted that an interference with freedom of expression can arise where age assurance is disproportionate, involves considerable friction, or requires excessive re-assurance by end-users (e.g. verifying their age every time they visit the same website). In line with the recommendations of the external study, the proposed Regulation allows service providers to adopt a successive validation approach, whereby service providers need not subject an end user to an assurance process if it has good grounds to believe the end-user meets the age baseline for access to a service or risky features (e.g. owing to the age of the account). Moreover, the proposed Regulation's focus on wallet-based solutions can capitalise on advancements in reusability and interoperability of age tokens, further reducing the friction and 'assurance fatigue' that of-age end users might be subjected to.

Finally, as noted in the external study, much of the problematic freedom of expression interferences are borne out of data protection and privacy concerns: individuals choose not to engage with age assurance systems, or alter their behaviour following an age check, because of concerns of identification, tracking, and potential data misuse. By ensuring the legislative instrument requires the use of the the EU Age Verification Solution to verify the age for the purpose of the access delay and comparative state-of-the-art privacy-preserving approaches (as noted in section 4.2.2) in the other instances, these concerns are directly addressed.

At the same time, the proposed Regulation strengthens children's freedom to information. By ensuring that reporting systems are age appropriate and accessible to children, children are empowered to report, contributing overall to a safer online environment. Similarly, child-friendly support tools contribute to a healthier environment and point children to diverse sources and advice that can help them navigate the online environment safely.

As for AI companions and general conversational chatbots, the safeguards listed in the proposed Regulation support children's right to seek and receive information, and to communicate and express themselves freely, including through AI companions and general conversational chatbots. The proposed Regulation does not aim to prevent minors from using such systems as tools for learning, accessing information, asking questions, or expressing thoughts and feelings. Rather, by establishing safeguards the proposed Regulation seeks to ensure that children can benefit from these technologies without being exposed to harmful content, manipulative interactions, or emotionally risky design. Furthermore, the requirement of the proposed Regulation to put safeguards on features of the system displaying behaviours or simulating emotions or interpersonal relationships, seeks, inter alia, to ensure child's right to receive information and form independent opinion. If an AI companion influences a child in hidden or emotionally persuasive ways, this may interfere with the child's ability to form independent views and decisions. Safeguards set by the proposed Regulation thus help prevent undue influence and preserve personal autonomy.

Overall, the proposed Regulation protects privacy-related freedom of expression and reinforces children's access to information.

4.2.4. Non-discrimination (Art 21 of the Charter)

Enhancing the protection of minors online will have a positive impact in mitigating risks for children in vulnerable situations and vulnerable groups to be exposed to discriminatory

behaviours. Safety by design obligations, in particular related to recommender systems and how children can influence their functioning in their best interest, will address certain discrimination concerns related to how certain online platforms amplify information and how the visibility of more extreme content or behaviours, including negatively affecting minorities or marginalised communities, can be maximised. These obligations will further empower children to better understand and have increased agency over those systems.

As noted in the external study, age verification solutions typically require the end-user to present a qualifying hard identifier – normally a passport or a national ID card – to enrol in the system and secure a digital proof of age attestation. In theory, this requirement could unfairly exclude individuals who lack qualifying hard identifiers or who lack the prerequisite technology to perform remote enrolment (i.e. a smartphone with an in-built NFC chip).

Member States can address this risk by provisioning national-level 'manual' enrolment mechanisms for those unable to enrol through the 'digital-first' approach. Most Member States already offer the possibility of enrolling in their national digital identity schemes via an in-person visit to a local municipal office or registry service, where the process can be completed 'manually'. This 'manual' enrolment fall-back option should be offered by deployers of the EU Age Verification Solution and comparative age verification solutions.

With respect to age-appropriate design, it is likely that some services will choose to deploy facial age estimation (FAE) as a means of assuring the age of users. FAE systems can pose risks of algorithmic bias. They are also typically less effective at estimating the age of individuals within the 13-17 age range as they are for the 18-25 age range, and there is a risk that some of-age users who fall within the system's 'buffer zone' will fail the age check. However, as noted in the external study, recent independent evaluations of facial age estimation have demonstrated continuing improvement in the accuracy and inclusivity of this method. And where age assurance is deployed in the market today, it is typical for service and systems providers to deploy successive validation or orchestration approaches to reduce concentration and exclusion risks that can arise from reliance on one method of assurance.

Finally, the proposed Regulation sets a high baseline for how age assurance deployments should ensure accuracy, reliability, and non-discrimination, among other outcomes. As noted in the external report, certain methods of age assurance, notably competence-based assessments, can be discriminatory against end-users who do not meet the assumed competency level that the age assurance deployer associates with their age group, for example, owing to a neurodivergence, age-related cognitive decline, or a medical condition impacting cognitive function. By setting a high standard for age assurance solutions, and by therefore foreclosing services from deploying problematic methods of age assurance to achieve compliance with the proposed Regulation's requirement, greater protection for the right to non-discrimination is ensured. To further limit potential exclusion, providers must offer effective and free of charge internal complaint-handling mechanisms that allow users to appeal incorrect age assessment.

4.2.5. Proportionality (Art 52 of the Charter)

As enshrined in Article 52 of the Charter, the principle of proportionality is crucial to ensure that any EU regulation strikes a fair balance between pursued policy objective of protecting children online and all the fundamental rights enshrined in the Charter affected by the measures to achieve it. The principle of proportionality is assessed through the tripartite test of whether the measures envisaged are suitable to effectively achieve the legitimate policy objective goal, whether the measures are necessary, i.e. the least restrictive of other rights that are available to

attain such policy goal, and whether different interests and rights have been balanced adequately in the choice of the measures in question.

The protection of minors online is a key policy objective of the Union. As explained in this section 4.2 and in section 2, as well as in view of initiatives of Member States and the Report of the Co-Chairs of the Special Panel, the proposed age restrictions, safety by design requirements and requirements related to age assurance for their implementation would represent necessary and suitable measures to ensure the protection of children's rights in the digital environment, which is currently insufficient and rapidly emerging as an urgent public health and safety risk for children to be addressed, as well as proportionate in view of the limited restrictions to some of the fundamental rights impacted by the measures, including those of children as explained in section 4.2.1. As outlined in this section, the risks of disproportionate restriction to children's rights in the Union are mitigated in the proposed Regulation by the gradual approach to imposing age restrictions to minors, enshrined in the possibility of minors to access accounts on safe services with the support, supervision and consent of their guardians, thus leading to autonomous use of safe services in line with their evolving capacities, as well as by the combination of such age restrictions supported by age assurance with safety by design measures protecting the privacy, safety and security of children. Similarly, possible risks of disproportionate impacts of age assurance measures on fundamental rights of all citizens in the Union are mitigated by the establishment of strict requirements for the implementation and operation of such age assurance methods, which must abide to the highest standards of accuracy, reliability, security, robustness, non-intrusiveness, privacy, and non-discrimination.

4.3. Economic Impacts

4.3.1. Overall Assessment

The proposed Regulation is expected to have an overall limited to moderate economic impact. The safety by design requirements largely codify existing Article 28 DSA obligations for online platforms and should therefore lead only to incremental costs for providers already broadly aligned with the DSA guidelines on protection of minors. The proposed Regulation creates an unambiguous compliance framework, which increases legal certainty, reduces fragmentation and enables more efficient enforcement. Without the proposed Regulation, providers would likely face up to 27 different sets of age restrictions and safety by design rules (see section 2.1). The rules would likely not just differ widely in terms of scopes and ages, but also include different parental control derogations, different technical requirements for age assurance, interface design, and monitoring as well as multiple enforcement structures. Such fragmentation would be extraordinarily burdensome, especially for the smallest providers with limited resources to familiarize themselves with a multitude of a different requirements and to implement them separately for each Member State. This would severely complicate the cross-border operation that is a defining feature of the digital economy ([326],[327]).

While much of the proposed Regulation builds on the guidelines on protection of minors, it also includes targeted additions that address residual protection gaps identified by the Report of the Co-Chairs of the Special Panel. The main additional costs are likely to arise from age assurance measures – for compliance with the minimum age rules and ensure safe designs and settings for minors – as well as safety by design adjustments, and the extension of certain obligations to AI companions and general conversational chatbots, online games and small and micro

[326] DSA Impact Assessment.
[327] DMA Impact Assessment.

enterprises. It is difficult to precisely determine the costs of these adjustments, especially for the potentially large number of small and micro providers of online services and online games that were previously not subject to Article 28 DSA. However, many of the costs are one-off design expenses for making services and systems safe for children. Recurrent costs are likely much more limited and primarily linked to maintenance and potentially marginal costs for age-assuring new accounts via third-party tools. Furthermore, those costs are mitigated by the development of the EU Age Verification Solution, the expected increased development of the market for safe design solutions, the fact that similar requirements already exist in EU law and increasingly in third countries and the avoided fragmentation of the internal market. This harmonisation, greater legal certainty, and public health benefits are expected to offset part of these costs over time.

4.3.2. Direct Compliance Costs for Providers

4.3.2.1. Providers Already Broadly Aligned with the Guidelines on the Protection of Minors

The proposed Regulation should be understood as a natural evolution of the guidelines on the protection of minors online following the recommendations of the Special Panel, rather than as a fundamentally new compliance paradigm. For services covered by the DSA, which are a substantial share of those in scope, the proposed Regulation is specifying Art. 28 of the DSA and relying on the enforcement structure of the DSA. Its core obligations follow the same protective measures that providers were already expected to implement under Article 28 DSA.. By turning these expectations into binding rules, the proposed Regulation is expected to increase legal certainty, reduce fragmentation, and support more consistent enforcement across the Union, without codifying every detail of the guidelines on the protection of minors.

This continuity runs throughout the proposed Regulation. For example, the guidelines already state very clearly that minors should not be exposed to design features that may lead to overuse or compulsive behavioural habits (§ 61(b)) ([328]). They spell out examples of such features in great detail (§ 61(b) and 57(b)) and call for concrete measures to be implemented, such as providing high safety settings by default, avoiding certain interface designs or offering effective time management tools (§ 61(c)), as well as easy to use, access and interoperable tools for guardians (§81 and 82) ([329]). The proposed Regulation's article on addictive design codifies these expectations into clear and binding rules. Similarly, § 64–67 of the guidelines lay out the same expectations on the design of recommender systems that are encoded in the proposed Regulation's article on recommender systems. In addition, §18 of the guidelines sets out that online platforms should conduct a risk review. The proposed Regulation requires VLOPs to monitor, test and evaluate implemented measures as part of the risk assessments carried out under Article 34 of the DSA. Indeed, under Article 34 of the DSA, VLOPs are already required to identify, analyse and assess systemic risks to the rights of the child, the protection of public health and minors as well as physical and mental wellbeing ([330]).It should also be noted that VLOPs are already required to undergo annual audits at their expense under Article 37 of the DSA. Table 2 illustrates that the proposed Regulation's safety by design obligations appear to a great extent already in the guidelines on the protection of minors, with quite targeted additions.

[328] Guidelines on the protection of minors.
[329] *Ibid*.
[330] Information regarding the costs relating to risk assessments and audit reports for VLOPs can be found in the DSA Impact Assessment.

These overlaps suggest that, for diligent providers already substantially aligned with the guidelines, the proposed Regulation largely formalises practices that should already be in place. The most notable additions, the harmonised minimum age of 15 for certain services, clearer requirements for age assurance and guardian control tools are discussed below and remain largely within the logic of the guidelines and are consistent with broader global trends towards stronger child protection standards.

The proposed Regulation should therefore generate only limited, incremental burdens for providers that are already substantially aligned with the guidelines. In most cases, they are likely to stem less from entirely new operational obligations than from the need to translate existing practices into a clearer, enforceable compliance framework and to make any targeted adjustments required by specific new elements of the proposed Regulation. Additional short-term adjustments should be weighed against the longer-term cost savings associated with a clearer and more harmonised Union-wide framework avoiding fragmented national approaches.

In short, the proposed Regulation builds on – not replaces – the guidelines on the protection of minors. It retains their protective and proportionate logic while making it more predictable and enforceable. For businesses already compliant with the guidelines, the transition should be relatively smooth, with limited additional costs and the benefit of greater legal certainty across the internal market.

Table 2 Continuity with safety by design obligations in 2025 guidelines on the protection of minors and DSA Articles

Article of proposed Regulation	**Correspondence in guidelines on the protection of minors**
Art 5 – Notification and independent audit of a compliance plan	DSA Article 37 mutatis mutandis.
Art 8 – General safety by design	§ 17(c)-(d) (privacy-, safety by design; age-appropriate design,). Proposed Regulation makes clear that settings for minors apply unless age assurance establishes that a user is an adult.
Art 9 – Addictive design	§ 57(b)(vi), (vii), § 61(b)-(c) (persuasive design features aiming at overuse such as autoplay, endless scrolling, artificial notifications, time-limited rewards or streaks, time-management tools). Proposed article applies only to online platforms that are online social networking services and video-sharing platform services.
Art 10 – Recommender systems	§ 64–67 (testing, explicit over implicit signals, no off-platform data, reset, safe recommendation, non-profiling option, child-friendly explanations and controls). Proposed article applies only to online platforms that are online social networking services and video-sharing platform services.
Art 11 – Safe settings	§ 57–58, § 59(a) (safe defaults settings, e.g. geolocation, camera, push notifications, contact synchronisation, disabling harmful settings/features). Proposed article applies only to online platforms

Article of proposed Regulation	Correspondence in guidelines on the protection of minors
	that are online social networking services and video-sharing platform services.
Art 12 – Contact and interaction safeguards	§ 57(b), (vi), (x), § 59(b)-(e), § 78(d), (f) (no unsolicited contact, no account recommendations, visibility controls, blocking/muting, group consent, no hosting live streams). Proposed article applies only to online platforms that are online social networking services and video-sharing platform services.
Art 13– Safety and Security of economic transactions	§ 69(j)-(l) (transparency of transactions, excessive or unwanted spending, paid loot boxes). Proposed article applies only to online platforms that are online social networking services and video-sharing platform services.
Art 14 – AI companions and general conversational chatbots	§ 61(e)-(f), 69(e) § 72(h)-(i), § 91(a) (no auto-activation, no nudging, opt-out, safeguards on commercial practices). Proposed Regulation adds rules on addictive designs, on safe settings, as well as restriction on features of AI systems displaying behaviours or simulating emotions or interpersonal relationships that are likely to create emotional dependencies.
Art 15 – Online games	§ 57–58, § 59, §61(b), § 78 (safe defaults settings, visibility, unsolicited contact, addictive design),. Proposed Regulation extends rules to online games.
Art 16– App-store obligations	General support in § 17, § 25–53 for age-based access restrictions and age assurance. Proposed Regulation adds specific app-store regime (age-rating, developer declarations, age assurance).
Art 17 – Codes of conduct on age rating	§ 17(a), § 84(c) (high standards, stakeholder cooperation, exchange of good practices). Proposed Regulation adds Union-level code with common criteria, mutual recognition, monitoring.
Art 18 – Agency of minors	§ 57(g), § 61(d), § 67(a), § 77, § 90–91 (child-friendly information, controls, feedback tools, warnings, temporary settings, transparency).
Art 19 – Child-friendly reporting and support tools	§ 75–77, especially § 77(a)-(f), § 78(a)-(d) (accessible, prioritised, confirmed, statement of reasons, explained reporting, blocking/muting, support links, helplines, warnings).
Art 20 – Guardian tools	§ 79–82 (age-appropriate, easy-to-use, privacy-respectful tools, time-management/settings integration, interoperability). Proposed Regulation adds non-circumvention, reporting mechanisms and refines interoperability for VLOPs.

Article of proposed Regulation	Correspondence in guidelines on the protection of minors
Art 20 – Collective complaints	DSA Articles 53 and 86.
Article 21 – Monitoring for VLOPs	§ 18 (risk review) and DSA Articles 34 and 35.

4.3.2.2. Age Assurance Requirements

Scope of the obligation and cost-mitigation features
Age assurance is likely to represent the most significant incremental compliance cost for some providers. As explained in section 3.2.4, the proposed Regulation may require age assurance measures for a range of reasons. In principle, this could lead a large number of services to require age assurance measures. It is difficult to accurately predict which online services and systems will prefer to implement age assurance measures rather than applying safe features and settings to all new, recently created and logged-out users, partly because it is difficult to predict demand for adult features and settings.

In any case, several mitigation measures are in place. First, the strict age verification methods are only required for social networking services and video-sharing services ~~and AI companions,~~ while the safety by design obligations and the obligation for providers of software application stores allow alternative age assurance methods. As noted in the external study, age verification systems – notwithstanding the availability of the EU Age Verification Solution – are typically more expensive to operate than alternative age estimation systems. As such, targeting of the strict age verification requirements and the obligation to rely on an EU Age Verification solution to a small subset of services for the purpose of the access delay, while enabling a broader range of assurance methods for the safety by design obligations, will ensure compliance costs are proportionate to the level of risk involved ([331]).

Second, existing accounts can be exempted where the provider can determine with a high level of confidence or based on the year of account creation that the account belongs to an adult. The external study found a strong preference for 'successive validation' techniques within the age assurance ecosystem. 'Successive validation' is an age assurance deployment approach under which end-users seeking to access a restricted service are subjected to the lightest touch, lowest-friction age assurance method first, and the system falls back to higher-friction, more invasive methods (e.g. age verification) only if the user fails to pass the prior age challenge. By enabling a form of successive validation, the proposed Regulation will significantly reduce both the compliance cost for companies and the friction involved in the age assurance process ([332]).

Initial deployment costs
Initial deployment costs are expected to vary depending on whether a provider builds an in-house solution or relies on a third-party provider. As the external study explains, proprietary in-house systems are likely to involve significant start-up costs, including code development,

[331] Bennett, O., 'Follow-up to recommendations on child safety online: analysis of the impact of age assurance on fundamental rights and the financial impact on the businesses concerned. A report for European Commission DG CNECT', 2026. [Bennett 2026]
[332] *Ibid*.

testing, training data, secure cloud storage, and legal, compliance and product policy costs. For that reason, the choice to develop a proprietary in-house solution is likely to be exercised only by the largest service providers, if at all ([333]). In practice, smaller and most medium-sized services are more likely to procure external solutions, which generally involve relatively modest set-up costs compared with proprietary system development ([334]).

Available evidence suggests that the costs of age assurance are generally manageable for most providers. The Australian government has estimated 80 hours of staff time per social media service to implement age assurance measures, a cost of EUR 0.39 per check per user and a total cost of about EUR 33 million to assure the age of 21 million Australians with 4 social media accounts each ([335],[336]). The impact assessment of the UK's Online Safety ACT assumes 12h of developer time for backend Yoti integration and estimates a ten-year total cost between EUR 21 million and EUR 107 million to assure the age of 27 million users per year accessing pornography ([337],[338]). It also notes that these costs are small compared to the costs of content moderation. In Ofcom's 2026 implementation findings set-up costs were in many cases reported to be modest, often in the range of tens of thousands of pounds, although some providers reported higher costs ([339]). Third-party providers themselves assert short implementation times of "approximately half a day" ([340]) to one week ([341],[342]). While these exact claims are not interpedently verified, the external study notes that for most small and medium-sized services, integrating third-party solutions is reasonably expected to cost in the hundreds of euros or low thousands of euros, although the evidence base remains limited ([343]). Online services applying age assurance measures also need to offer a complaint-handling mechanisms that allow users to appeal incorrect age assessment. The set-up costs for this are expected to very limited for most services since notice and action mechanisms are already required for all online platforms under Article 16 DSA, including for small and micro enterprises.

More broadly, the external study found that third-party age assurance vendors are increasingly competing on ease of deployment considerations, with some providers marketing their services as having internal integration costs that can be completed within hours and days. Many service providers will likely also benefit from lower deployment costs that stem from the fact that website builder platforms like WordPress and Shopify – platforms which many in-scope services utilise for business operations – facilitate low-friction plug-ins to third-party age assurance providers. In addition, the external study found increasing market interest in and optimism about the potential of interoperability of age assurance deployments, and how they could reduce compliance costs for services in the medium term. Projects like euCONSENT's AgeAware have created the technical and operational infrastructure through which age checks can be recognised across services and from which the costs of age checking can be shared. Interoperability innovations of this kind offer the further benefit of reducing the need for service

[333] *Ibid.*
[334] *Ibid*.
[335] Cost converted at AUD-EUR exchange rate as of 01/09/2026.
[336] Australian Government, Department of Infrastructure, Transport, Regional Development, Communications and the Arts, *Impact Analysis Equivalent Supplementary Analysis: OIA24-08210: Social Media Age Limit*, 2024.
[337] Cost converted at GBP-EUR exchange rate as of 01/09/2026.
[338] Department for Science, Innovation and Technology, '*Online Safety Act: Enactment Impact Assessment*', 2024. [OSA Impact Assessment]
[339] Ofcom, '*Report on the Use of Age Assurance*', 2026.
[340] OSA Impact Assessment.
[341] See https://didit.me/solutions/age-verification/
[342] See https://idenfy.com/integrations/
[343] Bennett 2026.

providers to invest in multiple different age assurance deployments to satisfy the preferences of their user base ([344]).

Taken together, these factors should relieve providers of some of the initial deployment costs – as well as the opportunity cost in terms of developer resource – that arise from the age assurance requirement.

Ongoing operational and per-check costs
The external study distinguishes between ongoing operational costs and per-check costs. Operational costs include legal, compliance, information security, customer support and supplier due diligence costs. These costs are likely to be lower where providers rely on third-party age assurance solutions rather than proprietary in-house systems, because much of the ongoing maintenance, operational security and due diligence is handled by the vendor. The available evidence does not suggest that such operational costs have prevented effective deployment.

In addition to the numbers cited in the section on initial deployment costs , Ofcom's 2026 implementation findings indicate that median per-check costs are low (around EUR 0.07) ([345]). They also suggest that per-check costs tend to decrease as the number of checks undertaken increases, with some large service providers understood to have faced per-checks costs of between EUR 0 and EUR 0.08 in other jurisdictions ([346]). Regarding operational costs, the Australian government has predicted that the required weekly staff time will fall from 10 hours to two hours after the first year, even for the very large providers subject to the Australian access delay. Overall, these findings suggest that age assurance is unlikely to constitute a prohibitive cost barrier for most providers, even if smaller services may face relatively greater implementation challenges. This supports the view that recurring operational costs, including per-check fees, system maintenance, compliance monitoring, and security safeguards, are likely to remain proportionate in most cases ([347]).

In the EU context, those costs may be further mitigated by the availability of the EU's open-source age verification solution, which is intended to lower implementation barriers and reduce dependence on proprietary commercial systems. This may be particularly relevant for SMEs and smaller providers, for whom up-front investment and procurement costs can be more difficult to absorb. The privacy-preserving and secure nature of the EU Age Verification Solution should further significantly reduce the ongoing maintenance and compliance costs that service providers would face were they to operate proprietary age assurance system. The study indicates that, over time, the EU Age Verification Solution is likely to be the cheapest means for providers to deploy age verification, because its development has been publicly funded and its technical architecture has been made available in open-source form, so those initial development costs need not be recovered from relying service providers on a per-check basis ([348]).

Recent experience in the UK offers an insight into the potential cost reduction benefits of the EU Age Verification Solution. While take-up of digital-ID-based age assurance solutions has been low under the UK's Online Safety Act (including in part, because there is no corresponding version of the open-source EU Age Verification Solution), the limited evaluation

[344] *Ibid*.
[345] Ofcom, '*Report on the Use of Age Assurance*', 2026.
[346] Bennett 2026.
[347] *Ibid.*
[348] *Ibid.*

data from Ofcom suggests that digital ID-based solutions are among the cheapest available to service providers on a per-check basis ([349]). In this respect, the EU framework may offer cost-reduction opportunities that are not fully comparable to the UK context reflected in Ofcom's evidence. The study therefore considers it reasonable to assume that providers relying on the EU solution are likely to face minimal ongoing per-check costs ([350]).

Longer-term market developments and broader compliance effects

It is important to note that the costs for age assurance should be seen against the clear expectation created by the guidelines on the protection of minors that providers take effective measures to prevent minors from accessing age-inappropriate services and experiences. Moreover, as noted in the external study, this proposed Regulation comes against a backdrop where age assurance – whether for corporate policy reasons or in response to existing regulatory requirements in the EU and third-countries – is becoming an increasing norm online for service providers ([351]). Indeed, for those providers that have already moved towards more robust age assurance in response to those guidelines and in response to other commercial and regulatory imperatives, the additional cost of the present proposed Regulation is therefore expected to be more limited, and mainly related to adaptation of existing systems, and compliance documentation. The study also points to evidence from the UK that some providers incurred no additional set-up costs because they already had commercial relationships and operational integrations with age assurance vendors in place ([352]). This is particularly relevant for very large platforms, many of which already operate age-related controls and are developing capabilities linked to the European Age Verification framework as well as age assurance requirements in other jurisdictions. Platforms that are subject to the minimum age and have not yet implemented the EU Age Verification Solution will face some additional costs.

The external study suggests that several broader market developments are also likely to place downward pressure on costs over time. These include growing competition among third-party vendors, developments in interoperability that may allow age checks to be recognised across services and costs to be shared, and the emergence of standards that can reduce the vendor due diligence burden on service providers. The study further suggests that, as age assurance becomes a more established global norm, providers operating across borders may increasingly benefit from economies of scale by amortising deployment and compliance costs across multiple jurisdictions. Rather than there being a settled 'consensus', the available evidence points to a reasonable expectation that age assurance costs are likely to decrease over time as the market matures and regulatory certainty stimulates further innovation and supply ([353]).

Last but not least, harmonised age assurance requirements at Union level are expected to reduce legal uncertainty and market fragmentation, thereby lowering long-term compliance burdens, especially for providers operating across multiple Member States. While the introduction or upgrading of age assurance systems may entail initial adjustment costs, a more consistent regulatory framework would reduce the need to adapt services to divergent national approaches and should therefore generate efficiency gains over time.

[349] *Ibid*.
[350] *Ibid.*
[351] *Ibid*.
[352] *Ibid.*
[353] *Ibid.*

4.3.2.3. Extension to additional entities and additional obligations for specific types of services and systems

The extension of certain protection-of-minors obligations to small and micro enterprises, app stores, AI companions and general conversational chatbots and online games, as well as minimal obligations on operating systems is expected to generate additional compliance costs for providers that are currently exempt from Article 28 DSA. Those costs may be relatively more burdensome for smaller providers because they have less internal legal, compliance and engineering capacity and fewer possibilities to spread fixed costs across a large user base. At the same time, the overall impact should remain manageable, in particular because the obligations are targeted, subject to proportionality, and in several respects reflect measures that responsible providers should already be considering where their services and systems are likely to be accessed by minors.

Small and micro enterprises

Including small and micro enterprises is justified by the nature of the problem. Exposure of minors to harmful content, contacts or design practices is not confined to large services. Available evidence indicates that harmful material and unsafe interactions can also be prevalent on smaller services, including niche or fast-growing services ([354]). Moreover, in digital markets, turnover or headcount is not a reliable proxy for societal reach or risk exposure. A relatively small provider may still attract very large numbers of users, including minors, in a short period of time, or may offer functionalities that create particularly significant risks. Exempting smaller providers altogether would therefore risk undermining the effectiveness of the initiative, creating incentives for risky activity to migrate towards less regulated services and systems, and weakening the objective of ensuring a consistently high level of protection for minors across the internal market. For the same reasons, the UK's Online Safety Act extend to small and micro enterprises as well ([355]). To ensure proportionality, very specific exemptions were provided on AI regarding the obligations for post-market monitoring may be particularly burdensome for small and micro enterprises.

For small and micro enterprises, the main cost drivers are likely to be age assurance, where relevant, as well as safety by design changes, such as the introduction of child-friendly reporting and support as well as default-setting mechanisms. In practice, however, many smaller providers are unlikely to develop bespoke systems. They are more likely to rely on third-party age assurance, moderation, parental consent or interface solutions, which limits the need for major in-house technical investment. Indeed, as noted in the external report, the market for third-party age assurance solutions is growing at pace, with providers increasingly competing on privacy, usability, and ease of deployment. So-called 'plug-and-play' solutions and ready-made integrations with website builder platforms like WordPress and Shopify are a market-driven response to the specific needs of small and micro-enterprises. This reality, allied with advancements in interoperability should insulate small and micro-enterprises from significant costs under this proposed Regulation. Small and micro-enterprises will further benefit from the availability of the EU Age Verification Solution, which significantly reduces the implementation and operational costs of age assurance ([356]). The availability of shared tools, vendor services and the EU Age Verification Solution should help reduce implementation barriers. For many providers, the main burden is therefore likely to consist of one-off integration

[354] The Internet Watch Foundation (IWF), *Online Harms White Paper Response*, 2021.
[355] OSA Impact Assessment.
[356] Bennett 2026.

and product-adjustment work, combined with ongoing but more limited costs related to maintenance, documentation and annual testing, monitoring and evaluation.

Finally, it must be emphasized again, as highlighted in the external study, that a single, harmonised EU framework is considerably cheaper for smaller providers to comply with than a patchwork of 27 national regimes and technical requirements ([357]).

Software application stores and operating systems
The proposed Regulation also requires providers of software application stores to put in place an age-rating system that developers must use when submitting apps. The principal administrative burden therefore falls on the providers of the software application store who will need to operate the rating framework and implement the age assurance solution. Developers may have to provide age-related information through a short questionnaire as part of the standard app-submission procedure, which is expected to represent only a marginal increase in workload relative to the overall app publication process.

Besides the direct administrative effort, developers may incur indirect costs if age rating process step leads to delayed approvals or if legitimate users are unable to complete the age check, potentially reducing downloads. This risk is mitigated by allowing a range of possible age-assurance options. While the new duties could increase the market power of app-store providers, this is mitigated by drawing up codes of conduct for age-rating systems that aims to harmonise labels and to ensure mutual recognition and consistent application of the ratings by online-platform providers throughout the internal market.

On the positive side, the codes of conduct will likely reduce collective costs of age ratings. On the developer side, a common age rating system across app stores significantly lowers costs as it eliminates the need to handle several age rating systems and better facilitates multihoming. This simplified entry also benefits app stores by increasing the number of available applications, in addition to the benefits of reduced efforts to developing and updating age rating methodologies and greater legal uncertainty. Common standards also help consumers navigate app stores, which in turn may benefit developers and app stores through increased downloads. Overall, the additional compliance requirements are expected to be manageable and to contribute to a higher level of protection for minors without imposing disproportionate burdens on developers or app-store operators.

The obligations on operating systems are minimal and only require providers to share relevant age signals they have obtained. This concerns only a small number of entities and builds on existing architecture for sharing OS-level information. Hence, the necessary adjustments are expected to be minimal. On the other hand, this provision may reduce age assurance costs for other providers by avoiding repeated age assurance. The obligation therefore seems very likely to be net beneficial.

AI companions and chatbots
The proposed Regulation is likely to generate compliance and redesign costs for providers of AI systems in scope, particularly chatbots and AI companions accessible to minors. The providers would need to invest in age assurance and age-appropriate safety by design features, such as safer default settings, and time-management tools.

Additional costs may arise from adapting user interfaces to remove nudging practices, restricting features of the system or behaviours that are likely to create emotional dependencies

[357] Ibid.

for minors, and putting in place governance, testing and monitoring processes. This may also constrain some engagement-based business models and reduce monetisation opportunities based on prolonged interaction. These requirements may weigh more heavily on smaller providers of chatbots and AI companions, however, they could also create demand for compliance technologies, age-assurance solutions and child-safety engineering services.

Several factors mitigate these costs. First, large parts are one-off design expenses for making services and systems safe for children. Recurrent costs are likely much more limited and primarily linked to the maintenance of these systems and potentially marginal costs for age-assuring new accounts via third-party tools, which are likely to be decreasing and quite limited as described above. Second, providers would likely face these obligations under national legislation and harmonized rules avoid much larger cost of implementation of fragmented and inconsistent technical requirements and makes scaling across Member States far easier. Third, the requirement to carry out post-market monitoring to identify, assess and mitigate emerging risks to the privacy, safety and security for minors, would not apply to micro and small enterprises.

Online games
The proposed Regulation is likely to generate one-off adaptation costs for affected providers of online games.Some obligations in the proposed Regulation would require on-going costs such as Article 14(1) point (a)for providers of online games continuously updating the video game with new content or features after release and for online gaming platforms to comply with the general obligations in section VI. Business organisations have thus reported risks of substantial impacts as off-by-default requirements or restrictions for minors could affect existing monetisation models and gameplay of their products. Industry has also noted existing consolidation pressure for small and micro-enterprises, which are estimated to represent around 80% of EU video game companies ([358]).

On the other hand, existing evidence of the Commission suggests that the impacts of relevant measures could be offset by the gains in terms of reputational risk as well as simplification savings for the companies. Furthermore, only a quarter of online game users in the EU are minors ([359]). This would indicate that if these functionalities are limited or prohibited only for minors or for minors under a certain age, the overall revenue may not be substantially affected as minors do not represent a large share of expenditure on video games.

Overall, it is important to emphasize that a harmonised Union approach is expected benefit to benefit all providers and in particular smaller providers operating across borders ([360]). In the absence of clearer common rules, providers may face divergent national expectations, greater legal uncertainty and duplicated compliance efforts. A more uniform framework should reduce those frictions over time and support the emergence of standardised technical and organisational solutions, including outsourced compliance tools tailored to smaller services. The proposed Regulation also allows for the creation of codes of conduct to be developed with the involvement of providers which could, where appropriate, build on existing pan-European age classification frameworks. Overall, while the extension of obligations to small and micro enterprises, app stores, online video games and AI companions and general conversational chatbots will entail additional costs, these are expected to be proportionate to the risks addressed

[358] European Commission, *The European media industry outlook – May 2023.*
[359] Video Games Europe & EGDF, *Facts about the European Game Industry*, 2024, p.8.
[360] DSA Impact Assessment.

and manageable in light of the targeted nature of the measures, the availability of external solutions, and the benefits of harmonisation and more level competitive conditions.

4.3.2.4. Safety-by-Design Adjustments

As pointed out above the saftey by design obligations largely appear already in the guidelines on the protection of minors**Error! Reference source not found.**. Besides the inclusion of additional entities and the clearer age assurance requirements, the main additions to safety-be-design are the following: The proposed Regulation requires all services and systems in scope to implement effective, accessible and user-friendly tools for guardians that are not easily circumvented or undermined and that offer a range of minimum functionalities. It also restricts AI companions and general conversational chatbots from exposing minors to design features and system behaviours that are likely to create emotional dependencies, formalises a right to collective complaints and encourages codes of conduct for harmonised age ratings. Potentially the most significant, but one-off, cost concerns the implementation of appropriate guardian tools. Providers will need to integrate functionalities such as time-management controls, editing of settings related to privacy, contact, visibility, notifications, geolocation or camera, and to reporting harmful content, accounts or behaviour on behalf of their child. Once these features are built or sourced from third-party solutions, the remaining expenses should be largely limited to periodic maintenance and updates.

Restricting AI companions and general conversational chatbots from exposing minors to design features and system behaviours that are likely to create emotional dependencies create additional compliance costs for providers, but these costs are likely to be proportionate to the underlying risk. In practice, the providers would need stronger ex-ante evaluations to assess whether design features (such as, e.g., persistent personalisation, relational language, emotional mirroring), could foster harmful attachment. Post-market monitoring, which do not apply to micro and small enterprises, would also need to be reinforced through incident reporting, periodic review of interaction patterns, and processes to detect harmful or manipulative outcomes once systems are deployed. For providers, this may increase development and operational costs, lengthen time to market, and require redesign of engagement strategies that currently rely on maximising user retention through relational features.

Regarding the prohibited features of the chatbots and companions, some examples of exploitative and manipulative practices could possibly already be covered under the prohibitions under the AI Act, thus making the costs marginal. Furthermore, many providers have already been implementing safety measures and mitigations in response to the ongoing investigations and litigations in hundreds of cases in the US on harms suffered by minors and other persons from chatbots and companions ([361]). Similar safety by design measures are also required in mandatory legislation introduced in various US states on the protection of minors from harms and risks posed by chatbots and companions ([362]). The impacts of relevant measures would also be offset by the gains in terms of reputational risk as well as simplification savings for the companies. The costs are therefore expected to be proportionate to the risks addressed and manageable in light of the targeted nature of the measures and the benefits of harmonisation and more level playing field.

[361] Whitford, E and Miller, A., 'AI chatbots offer next front for US state AGs following Meta settlement', *MLex*, 26 August 2026; Six, T., 'Manipulative technology: Kentucky sues AI chatbot company for endangering children', *Lexington Herald Leader,* 8 January 2026.

[262] California's SB 243 (2025), Companion Chatbots; New York General Business Law, Article 47 - Artificial Intelligence Companion Models; Utah HB 438 - Companion Chatbot Safety Act.

As the codes of conduct are facilitated by the Commission and participation of firms is voluntary, this article is not expected to create substantial costs for businesses and instead create benefits from improved harmonisation. The collective-complaint mechanism already exists under Article 53 DSA. For services and systems newly in scope, this obligation merely adds a procedural channel for complaints lodged with regulators and therefore does not create material implementation costs or entry-barriers. For safety by design obligations that largely replicate the provisions in the guidelines on the protection of minors, most providers are expected to only require modest, one-off product redesigns or adaptations to ensure formal compliance with the clarified and binding design requirements. Typical adjustments may involve changing default settings, disabling certain features such as autoplay or modifying recommender-system signals. The associated costs are expected to be comparatively small.

It is important to recognise that, although the absolute financial impact will be lower for small and micro enterprises because their products are less complex, the relative burden may be higher for these firms. Smaller providers have more limited legal, compliance and engineering capacity and therefore may find even modest integration and monitoring tasks proportionally demanding. Nonetheless, the harmonising effects of the proposed Regulation are expected to stimulate the development of open-source UI components and standard practices for child-safety features. In the context of the Online Safety Act, the UK government observe continued growth in the UK's safety tech sector and notes an "ongoing trend for 'Safety Tech as a Service (STaaS)'" ([363]). Falling development costs – partly driven by more efficient coding tools ([364]) – are expected further reduce the financial and technical effort required to comply, especially for smaller providers.

The redesign and compliance costs are expected to be higher for providers whose current service design is not yet aligned with child-protection-oriented practices. However, this should also be seen in light of the fact that some of the practices concerned may already be difficult to reconcile with existing Union consumer, data protection and DSA requirements where minors are affected. To the extent that the proposed Regulation requires providers to discontinue or redesign features that depend on manipulative or otherwise harmful engagement techniques, this may reduce revenues derived from business models that are not consistent with the Union acquis or with the protective logic already underpinning Article 28 DSA. From that perspective, part of the economic effect is not a new regulatory burden in a strict sense, but the removal of advantages enjoyed by providers that have not yet internalised the costs of safer design. This can improve competitive conditions for providers that already invest in compliant and child-safe services and systems.

4.3.3. Costs for Member States

Overall, EU Member States are expected to face additional administrative, technical and enforcement costs, although these are expected to remain moderate. These costs would primarily be linked to ensuring the availability for their citizens of at least one EU Age Verification solution and means of obtaining proof of age attestations, of parental responsibility, supervising the additional entities covered by the proposed framework, and implementing the flanking national measures to support child safety. However, Member States would have faced some of these costs even without the proposed Regulation and are primary beneficiaries of the harmonisation effects, increased cross-border trade and the expected public

[363] Department for Science, Innovation & Technology, *UK Safety Tech Sector: 2025 Analysis*, 2025.
[364] Zheyuan Cui, K., et al., 'The Effects of Generative AI on High-Skilled Work: Evidence from Three Field Experiments with Software Developers', *Management Science*, 0(0), 2026.

health benefits. Furthermore, increased coverage and use of digital identity solutions will also bring wider benefits for e-governance beyond online child safety.

The proposed Regulation requires Member States to ensure the availability for their citizens of at least one age verification solution and of different means of obtaining a proof of age attestation. It is important to note that this is an obligation to ensure practical availability, not necessarily to design, develop, finance or operate a public solution. It could be met through a public solution, an eIDAS-based route, a procured private service, the use or recognition of a cross-border solution, or a hybrid model. The magnitude of the costs will therefore depend on the implementation choices made by Member States and on the extent to which existing infrastructure and market solution can be used. Member States would nevertheless face administrative tasks: mapping available solutions, ensuring that at least one route is operational, addressing accessibility gaps, facilitating cooperation and cross-border availability, and supervising providers in scope. Competent authorities may also need technical expertise to evaluate equivalence claims, investigate complaints, assess whether updates have lowered performance, and coordinate with data-protection, consumer-protection, cybersecurity and eIDAS authorities. Many of these costs are expected to be mitigated through cooperation and joint technical capacity, templates, published criteria and standard evidence packages.

It is essential to note that Article 5 of the European Digital Identity Regulation already required every EU Member State to provide at least one EU Digital Identity Wallet to all citizens, residents, and businesses by 2026, ensuring interoperability, privacy, and secure access to digital services across the EU ([365]). The EU Age Verification solution can be integrated relatively easily into the Wallet. While it has to be certified separately and published on the trusted list under the EU Age Verification Scheme, the costs associated with integrating the age verification functionality into existing digital identity infrastructure are expected to be lower than the costs of establishing such infrastructure in the first place. In practice, the costliest obligation could be ensuring the availability of in-person verification options or digital identity-based onboarding methods to ensure that individuals without a passport or electronic ID card, or without an NFC-enabled smartphone, can verify their age. These costs largely depend on the coverage of existing digital identity and in-person verification solutions in the Member State and the coverage of 15-to-17-year-olds with the necessary identity documents. In most Member States, minors can already obtain ID cards from the age of 15, and many Member States already operate digital identity solutions, at least for adults. To limit costs, additional coverage could be targeted rather than requiring universal public provision. While costs are proportionately higher in Member States with more limited existing infrastructure, increased coverage will bring clear benefits beyond online child safety, notably for e-governance and digital administration services.

The proposed Regulation also includes flanking national measures to prepare and support minors, notably ensuring easy, free and confidential access at national level to channels through which minors can seek assistance in relation to the harms, as well as awareness raising activities. However, these measures very closely follow existing initiatives, notably the action plan against cyberbullying as well as the Better Internet for Kids strategy and its network for Safer Internet Centres and should imply at most limited marginal costs ([366], [367]).

[365] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework, ELI: http://data.europa.eu/eli/reg/2024/1183/oj), Article 5a.
[366] Action Plan against cyberbullying.
[367] BIK+.

As discussed above, the proposed regulation covers additional entities compared to Article 28 DSA. Most smaller providers as well as online games that are video games are supervised by national authorities, which may lead to additional enforcement work. However, enforcement builds on existing DSA and AI Act enforcement structures, limiting marginal costs. Importantly, Member States would have faced many of these costs, and potentially more, without the proposed Regulation. As described in detail in section 2.1, most Member States are working on national regulatory initiatives that would lead to additional enforcement obligations. For instance, the Austrian proposal was estimated to require additional staff equivalent to 0.5 full-time equivalents, i.e. EUR 60,000 ([368]). Among other tasks, Member States would have had to assess existing technology and requirements for age verification, access restrictions and safety by design and take official action in case of serious infringements. National authorities themselves have repeatedly suggested extending obligations to small and micro enterprises, notably in the context of Working Group 6 of the European Board For Digital Services. The impacts on public authorities are further discussed in section 4.3.4.2 below.

At the same time, Member States will gain several economic benefits from the proposed Regulation. By harmonising age-verification and safety-by-design rules across the Union, it is expected to reduce the need for national regimes. Much of the legislative, technical and enforcement effort that Member States would have otherwise incurred are thus avoided or reduced, while certain common technical and implementation task are undertaken at Union level. Moreover, the benefits of strengthening the internal market and fostering cross-border trade (see 4.3.4.1) as well as the potential benefits from boosted innovation in the digital space (see 4.3.4.3) accrue primarily to the Member States. Similarly, the proposed Regulation's public-health objectives – including a reduction in the incidence and impact of online harms affecting minor – may translate into long-term savings for national health and social-care systems (see 4.3.4.4). Overall, the harmonised framework is expected to provide legal certainty, economic efficiency and societal benefits, while limiting the need for Member States to establish and maintain divergent national frameworks.

4.3.4. Broader Economic Effects

4.3.4.1. Internal Market

Beyond direct compliance costs, the proposed Regulation is expected to have broader economic effects that are overall limited to moderately positive, although some uncertainty remains as regards the scale and timing of those effects. A central consideration is the functioning of the internal market. In an area where several Member States are already moving towards national rules on age limits, access restrictions and age assurance, further Union-level clarification and harmonization of the protection of minors framework can reduce regulatory fragmentation and create a more predictable environment for cross-border service provision. This is particularly relevant for digital services and systems, which typically operate across borders and would otherwise need to adapt products, terms, technical systems and compliance processes to diverging national approaches. In that respect, the proposed Regulation is expected to generate the same type of harmonisation benefits that underpinned the DSA and the AI Act more generally: lower legal uncertainty, fewer duplicative adjustments and more level conditions of competition within the internal market. For the DSA, these were estimated to increase turnover generated cross-border by EUR 8.6 to EUR 15.5 billion ([369]). In case the DMA, the benefits from reduced fragmentation and increased cross-border trade were estimated to be EUR 92.8

[368] AT Impact Assessment
[369] DSA Impact Assessment.

billion and EUR 450 billion to EUR 1.76 trillion after 10 years respectively ([370]). While these effects are inherently difficult to quantify, this does suggest first-order economic benefits of the proposed new Regulation.

These benefits may be especially important for providers active in several Member States, including smaller firms seeking to scale across borders. In the absence of a clearer common framework, larger providers are generally better placed to absorb the fixed costs of legal analysis, technical adaptation and ongoing monitoring across multiple jurisdictions. A more harmonised Union approach can therefore help limit the extent to which fragmentation itself becomes a competitive advantage for the largest players ([371]).

4.3.4.2.Public Authorities

For public authorities, the economic impact is expected to be neutral and potentially slightly positive overall. Additional costs for regulators might plausibly be offset or outweighed by savings in the public health sector from improved mental and physical health.

The proposed Regulation likely requires additional spending on regulatory capacity, both at the national and EU level, for two reasons. First, there are new obligations to enforce, notably the minimum age and the more stringent age assurance requirements. Second, investigating compliance of for the potentially large number of small and micro providers could increase case load substantially, though it is expected that first-order compliance issues are rarer among these providers and that cases are less complex. Third, regulators will need additional resources to conclude investigations in the very short, envisaged time frames. Experience has shown that stable resources and permanent staff who are well experienced with both the regulation and the particular digital service or system under investigation are key to swift enforcement.

As a reference, the Australian Government has planned AUD 76.1 million (ca. EUR 47 million) over four years from 2024–25 (and AUD 16.9 million (ca. EUR 10.4 million) per year ongoing from 2028–29) to establish the minimum age of access to social media, including AUD 12.3 million (EUR 7.6 million) per year ongoing for the Office of the eSafety Commissioner to provide regulatory oversight and enforcement functions ([372]). The impact assessment of the UK's Online Safety Act has estimated costs to the regulator of GBP 62.6 million (EUR 73 million) per year ([373]) and for 2025/26 Ofcom has reported an increase in staff costs of GPB 16 million (EUR 18.7 million) and of ICT costs of GPB 3.7 million (EUR 4.3 million), both driven by regulation of new duties ([374]). Under the proposed regulation, part of the enforcement costs may be recouped via fees.

On the positive side, clearer obligations should make supervision and enforcement more efficient than in a situation where authorities and providers must rely primarily on broad principles and non-binding guidance. A more uniform framework may also reduce frictions linked to cross-border enforcement and reduce uncertainty for authorities as well as providers. Furthermore, to the extent that the proposed Regulation contributes to improving the mental and physical health of minors, it reduces public health care expenditure. Some economic

[370] DMA Impact Assessment.
[371] *Ibid*.
[372] Commonwealth of Australia, *Mid-Year Economic and Fiscal Outlook 2024–25*, 2024.
[373] OSA Impact Assessment.
[374] Ofcom, *Annual Report and Accounts 2025–26*, 2026.

estimates for the United States suggest that the health care cost alone for social-media related depression might be in the order of billions of dollars ([375]).

4.3.4.3.Innovation, Competition and the Digital Ecosystem

Overall, it is expected that the proposed Regulation supports innovation and level competition in the digital space. In principle, the proposed Regulation may create some additional barriers to entry, notably acquiring familiarity with the legal obligations, implementing the granular guarding control tools that are required for providers of all sizes and sectors and, where needed, age assurance measures to comply with safety by design requirements. This effect should not be overstated, but it is likely to be felt more acutely by smaller providers with limited in-house legal, engineering and compliance capacity, which could potentially impact innovation and market concentration in certain areas. Research has linked the GDPR to a substantial reduction in the number of apps available in EU app stores, citing administrative burdens, increased developer cost, reduced revenue and lack of knowledge of obligations, with stronger effects for fringe applications ([376]). While some of these concerns apply to the proposed Regulation, the concerns are mitigated by several factors. First, the testing, monitoring and evaluation obligations apply only to very large online platforms, limiting the administrative burden for smaller providers. Second, the strictest age assurance requirements (age verification) are limited to social networking and video-sharing platforms and AI companions only.

Some business models may also be affected more directly where they depend on design choices that maximise engagement in ways that are difficult to reconcile with a high level of protection for minors. To that extent, the proposed Regulation may reduce revenues associated with certain practices for some providers. However, this should be seen in context. Where the proposed Regulation mainly clarifies and codifies the protective logic already inherent in Article 28 DSA and related guidance, part of the economic adjustment reflects the removal of advantages previously enjoyed by providers that had not yet internalised the costs of safer design. This will improve competitive conditions for firms that already invest in age-appropriate and child-safe services. Thus, the harmonised legal requirements would establish a level playing field across the single market.

There are two further reasons why the proposed Regulation is expected to boost innovation. First, it likely fosters innovation in child-safe digital services and systems. In particular, it can strengthen demand for privacy-preserving age assurance tools, safer default settings, child-friendly interface design, parental tools and other technical solutions that enable compliance while limiting unnecessary data processing. Over time, this may contribute to the development of specialised compliance and safety technology markets in the Union. In that context, synergies with wider EU digital infrastructure, including the EU Digital Identity Wallet and the Union's age verification solution, may help lower implementation costs and reduce dependence on proprietary systems. The extent of these benefits will depend on uptake and technical maturity, but such synergies could become more important over time, especially for smaller providers that rely on shared solutions rather than bespoke systems.

Second, it is important to emphasize the advantage of common harmonised rules again. The immense burden of 27 different national regimes imposing divergent requirement along a range

[375] See the lower bound estimate derived in the open-source online calculator: Team, S. S. R., *What might social media's mental-health effects cost society,* Accessed August 2026.
[376] Janßen, R., et al., 'GDPR and the Lost Generation of Innovative Apps', *National Bureau of Economic Research*, 2022.

of dimensions as well as legal uncertainty regarding concrete child safety requirements and the increasing number of related lawsuits have chilling effect on investment and can dissuade businesses from expanding and growing in the single market. The burden of different enforcement regimes and the costs for companies of dealing with multiple enforcement agencies are similarly prohibitive for smaller enterprises and thus hamper innovation. The harmonised measures would cut the costs of the evolving legal fragmentation, and the extended scope would fully level the regulatory playing field for online child safety in the EU. These benefits were also a key rationale for the DSA in the first place ([377]). More generally, a stable and predictable regulatory environment are generally seen as creating conducive to investment innovation ([378],[379]).

4.3.4.4.Indirect Long-Term Economic Benefits

Finally, to the extent that the proposed Regulation contributes to reducing online harms affecting minors, it may also generate indirect longer-term economic benefits that are not easily quantifiable in this assessment but are likely to be relevant. Research has found significant negative impacts of early social media use on learning outcomes in PISA tests ([380]) and indicated that online distractions can reduce productivity ([381],[382],[383]). Economic estimates for the United States suggest that the social cost of social media from depression, medical bills, lost work time and deaths could be as high as 2.4 trillion dollars ([384], [385]). A safer online environment may support better well-being and, over time, better educational and developmental outcomes for children. It may also reduce certain wider societal costs linked to harmful online experiences. These effects are inherently difficult to monetise and will depend on implementation and effectiveness in practice. Nevertheless, they point towards potentially important longer-term gains that go beyond the immediate compliance impacts on providers.

Taken together, the broader economic effects of the proposed Regulation appear manageable. The main negative effects are likely to arise from higher short-term costs for compliance checks, product redesign, and, for some firms, possible adjustments to business models. These effects should, however, be weighed against the expected benefits of greater harmonisation, improved legal certainty, more level competitive conditions, better enforceability and possible innovation in child-safe digital services and systems. On balance, the proposed Regulation is therefore not expected to give rise to disproportionate economic costs, while it may generate meaningful medium- to long-term benefits for the internal market and society more broadly.

---

[377] DSA Impact Assessment.
[378] World Bank, 'World Development Report 2005: a better investment climate for everyone'.
[379] Baker, S. R., Bloom, N., Davis, S. J., 'Measuring Economic Policy Uncertainty', *The Quarterly Journal of Economics*, 131 (4), 2016, pp.1593–1636.
[380] Gui, M., et al., 'Longitudinal Effect of Early Social Media Use on Standardized Learning Outcomes during School Career', *Nat Hum Behav*, 2026, pp.1–13.
[381] Ward, A. F., et al., 'Brain Drain: The Mere Presence of One's Own Smartphone Reduces Available Cognitive Capacity', *Journal of the Association for Consumer Research*, *2* (2), 2017, pp.140–154.
[382] Marotta, V., Acquisti, A., 'Online Distractions, Website Blockers, and Economic Productivity: A Randomized Field Experiment', *Preliminary Draft* 2017, 5.
[383] Lim, V. K. G., Teo, T. S. H., 'Cyberloafing: A Review and Research Agenda', *Applied Psychology*, *73* (1), 2024, pp.441–484.
[384] See the headline estimate based on the research baseline derived in the open-source online calculator. Team, S. S. R., *What might social media's mental-health effects cost society,* Accessed August 2026.
[385] Braghieri, L., Levy, R., Makarin, A., 'Social Media and Mental Health', *American Economic Review*, 112 (11), 2022, pp.3660–3693.

5. CONCLUSION

The proposed Regulation will deliver a single, Union-wide framework that safeguards children's health, well-being and fundamental rights while improving legal certainty for providers of digital services and systems in scope. By establishing a harmonised access delay of 15 years for social-networking services, video-sharing platform services and AI-companions, it prevents exposure to the most harmful design features during the critical phase of adolescent development and improves minors' mental and physical health. The accompanying safety by design obligations – prohibiting addictive mechanics, enforcing child-friendly default settings and guaranteeing transparent, controllable recommender systems – ensure that the services and systems which remain accessible are intrinsically age-appropriate, thereby protecting minors from compulsive use and unsafe content. Mandatory, privacy-preserving age-assurance mechanisms underpinned by the EU Age Verification Solution further guarantee that only users of the required age can create accounts, whilst offering parents robust supervision tools without compromising data-protection standards.

In parallel, the Regulation will avoid a patchwork of national rules, simplifying compliance for providers of all sizes and strengthening the single digital market. Uniform obligations reduce duplicated administrative burdens, lower compliance costs and enable more efficient, coordinated enforcement. This clearer legal environment will also encourage innovation in child-safe technologies, such as interoperable age-verification solutions and child-friendly interfaces, creating new market opportunities and strengthening the EU's global leadership on online child protection. Ultimately, the proposed Regulation delivers a proportionate, evidence-based response that enhances the safety of the online environment for all children and adolescents across the Union, creates a level-playing field for child-online protection, and supports the long-term social and economic benefits of a healthier, more resilient digital generation.

From the outset, the Commission has pursued an evidence-based approach to this initiative. As announced by President von der Leyen in her 2025 State of the Union address, the Commission launched this initiative by establishing a Special Panel of leading specialists to develop recommendations for a European approach to children's online safety. The panel brought together the latest knowledge from across health, neuroscience, psychology, computer science and child rights, alongside the experiences of children, young people and parents across the Union. Drawing on this broad expertise, as well as comprehensive input from stakeholders and young people, the Co-Chairs of the Special Panel on child online safety presented their report in July 2026.

The proposed Regulation presented by the Commission builds closely on the recommendations in the report of the Co-Chairs of the Special panel and reflects the Commission's evidence-based approach throughout the process. In the same spirit, the Commission intends to put in place a robust monitoring and evaluation framework to assess how the new rules operate in practice, whether they achieve their objectives, and whether any unintended effects arise over time. This will help ensure that implementation remains proportionate, effective and responsive to technological and market developments.

The evaluation approach will combine different sources of evidence and draw on the highest available expertise, including independent academic partners and relevant stakeholders, with appropriate attention to children's rights, privacy and research ethics. It will examine both implementation and outcomes, including the effectiveness of the access delay, the personal scope of the access delay, impacts on minors' exposure to online risks and harms, broader

effects on wellbeing and participation online, fundamental rights of minors and adults as well as possible consequences for parents, providers and the internal market. In doing so, the Commission will draw on relevant international experience, such as the ongoing Australian Social media age restrictions evaluation. The Commission also intends to ensure that children's and young people's perspectives are meaningfully reflected in this work, and to publish findings in a transparent and timely manner so that they can inform future review and adjustment of the framework. In this way, the initiative is designed not as a static intervention, but as a future-proof regulatory approach capable of learning from evidence and adapting as services, risks and user behaviour evolve.