Council of the European Union

Brussels, 18 September 2026
(OR. en)

13321/26

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

PROPOSAL

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.:	COM(2026) 681 final
Subject:	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 COM(2026) 681 final.

Encl.: COM(2026) 681 final

EUROPEAN
COMMISSION

Brussels, 17.9.2026
COM(2026) 681 final

2026/0286 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

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

{SWD(2026) 681 final}

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

Only half of children aged 9-16 across Europe say they feel safe online. The risks faced by minors online are real and urgent, and impact their health, development and wellbeing, such as for example reduced physical activity, increased risk of myopia and reduced sleep, depressive and anxious symptoms, decrease self-esteem, negative impact on learning and cognitive development, eating disorders, decreased empathy, loneliness and addictive behaviours. Minors online also face risks of cyberbullying, child sexual abuse and grooming.

The protection of minors online is a political priority of the Commission. In her 2025 State of the Union, Commission President Ursula von der Leyen announced that she will commission a panel of experts to advise her on the best approach for Europe on child safety online. After a process in the first half of 2026 involving a wide range of experts from different fields, as well as representatives from industry, parents and youth, the co-chairs of the Special panel presented their recommendations to the President in July 2026. The recommendations set out a clear path for enhancing the safety of minors online and ensuring the functioning of the Single Market. In particular, they recommend an EU-wide access restriction, harmonised safety-by-design rules as well as proportionate, privacy-preserving age assurance systems. Finally, they recommend covering digital services beyond social media platforms, including app stores, AI companions and some video games and video-sharing platforms offering risky features.

In October 2025, the Jutland Declaration signed by 25 Member States called for age verification and for a safer online environment for minors. In its conclusions of March 2026 and of October 2025, the European Council also stressed the importance of protecting minors online, including through a digital age of majority. In its report of November 2025 on the protection of minors online, 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 unless parents or guardians have authorised their children otherwise. It also called upon a harmonised European digital age limit of 13, under which no minor can access social media platforms. The European Parliament also recognised the need for additional legislation on age-appropriate design and safety by design. It further called for a European approach regarding age assurance ensuring legal certainty.

Across the European Union, Member States are discussing or proposing national legislation to enhance the safety of minors online. Italy, France, Norway, Greece, Austria, Poland and Belgium notified in 2025 and 2026 their draft legislation limiting access to certain digital services for minors under a certain age. Norway also notified its legislation in May 2026. In almost all other Member States, consultations are ongoing, drafts are discussed in national parliaments or have been announced by governments. Proposed national draft legislations differ in terms of scope, age limits and types of restrictions imposed, risking fragmenting the single market, reducing legal certainty and increasing compliance costs while providing an uneven level of protection for minors across the European Union.

The current online environment is not designed with minors in mind. While legislation already exists to create a safer online environment, no single legislation takes the children and their safety and empowerment as the starting point. Building on the key principles set out in Regulation (EU) 2022/2065 and Regulation (EU) 2024/1689, this proposal seeks to protect

minors from risky digital services and AI systems, uphold the digital single market and maintain a coherent regulatory framework and enforcement structure for the protection of minors online.

The proposal recognises the risks that minors face on certain online social networking services and video-sharing platforms and therefore limits autonomous account creation on those specific platforms and systems by children below the age of 15 years. By providing one age across the European Union, it harmonises diverging national rules removing obstacles to the implementation of the Digital Single Market, ensuring legal certainty and a similar level of protection for all children in the European Union. This is combined with rules that recognise the role of parents and legal guardians in supporting the safe development of minors online, by creating accounts with limited functionalities for minors on from 13 years as well as rules to create an environment of safe services and systems for very young children with strict parental supervision and which takes into account their development. In line with the developmental approach recommended by the co-chairs of the Special Panel on Child Safety Online, minors below the age of 13 should not have access to harmful online social networking services and video-sharing platform services.

The proposal sets out clear safety by design requirements for online social networking services, video-sharing platform services, online games, AI companions and general conversational chatbots, and software application stores. Building on the recommendations of the co-chairs of the Special panel, it harmonises and extends those requirements ensuring legal certainty across the Digital Single Market and a high level of protection for minors across the digital environment, taking into account that business models are constantly changing in this dynamic field and loopholes must be avoided.

To underpin the access delay and the implementation of safety by design requirements, the proposal establishes a clear framework for age assurance with clear criteria and safeguards for the use and deployment of such systems. By enshrining requirements for the use of age assurance methods, the proposal ensures that the use of those methods will be proportionate, effective, reliable and privacy-preserving. It also provides for common criteria for age assurance ensuring the functioning of the Single Market.

A fast, effective and robust enforcement is critical to the protection of minors online and the functioning of the Single Market. The proposal therefore lays out an enforcement framework that relies on existing enforcement structures while providing for a an expedited enforcement procedure.

- **Consistency with existing policy provisions in the policy area**

The proposal builds on the existing legislative framework for the protection of minors online ensuring the functioning of the Single Market. By building on Regulation (EU) 2022/2065 and Regulation (EU) 2024/1689, it provides continuity and coherence with the EU regulatory framework for digital services and AI systems while developing specific requirements for the protection of minors online taking into account their evolving capacities, safety and empowerment as a starting point.

This proposed Regulation is without prejudice to the Digital Services Act, and builds on the provisions laid down therein, notably on Article 28 regarding the obligation for certain providers of online platforms to take appropriate measures to ensure a high level of privacy, safety and security for minors. The proposed instrument, and in particular its provisions related to safety by design, set in “hard law” those specifications that the Commission has

already included in the Guidelines on protection of minors under Regulation (EU) 2022/2065. In doing so it specifies the obligations set out in Article 28 of Regulation (EU) 2022/2065 where these concern safety by design and age assurance requirements. Therefore, ongoing cases related to these obligations under Regulation (EU) 2022/2065, in particular Article 28, remain unaffected. The proposed Regulation is also without prejudice to Regulation (EU) 2024/1689 and builds on its framework, notably on its comprehensive risk-based rules. The proposed Regulation is complementary and does not affect the prohibitions and other obligations and requirements for AI systems and general-purpose AI models already established in Regulation (EU) 2024/1689.

The Better Internet for Kids strategy (BIK+) supports the implementation of this legislative framework, notably Regulation (EU) 2022/2065. Under the BIK+, the EU co-funded network of Safer Internet Centres offers training sessions, helplines and hotlines and run awareness raising activities. They regularly consult children and young people on their needs and view on online safety. In February 2026, the Commission adopted the Action plan against cyberbullying to prevent cyberbullying, raise awareness and make it easier to report and ensure that victims receive adequate support. The proposal is consistent with those non-legislative actions, and builds upon them to give kids in Europe the best support when they use the online environment.

- **Consistency with other Union policies**

The proposed Regulation introduces a horizontal framework for the protection of minors online. This Regulation is without prejudice to the rules laid down by other Union legal acts regulating other aspects of the provision of intermediary services in the internal market, in particular, the rules on audiovisual media services, consumer protection and product safety, and on the protection of personal data.

The proposal will be complemented by further actions which would be in full alignment with this Regulation, including the ongoing evaluation and upcoming review of the Audiovisual Media Services Directive that will additionally 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.

Furthermore, the upcoming Digital Fairness Act (“DFA”) aims at strengthening and making consumer protection law fit for purpose, also in the digital environment, in full alignment with the obligations in this Regulation. Consumer law plays an important role in ensuring that consumers, children in their consumer role included, are not exposed to unfair or misleading practices. The Unfair Commercial Practices Directive (“UCPD”) in particular acknowledges children as vulnerable consumers that need enhanced protection; it also bans a direct exhortation to children to buy advertised products or persuade their parents or other adults to buy those products for them. Furthermore, as part of the revision of the existing consumer protection law, the CPC Regulation will also be revised to strengthen the existing enforcement coordination system for national authorities and vest in the Commission direct investigation and enforcement powers in specific cases.

Additionally, the recent changes to Regulation (EU) 2024/1689 prohibiting AI systems generating child sexual abuse material, the on-going adoption of Regulation to prevent and combat child sexual abuse, together with the recently adopted Recast of the Child Sexual

abuse directive, strengthens the EU framework against child sexual abuse and exploitation, both online and offline. They will improve prevention, investigation and support for victims.

The proposal is also fully consistent and further supports existing or upcoming initiatives to empower and support minors and ensure their well-being online, including the EU Strategy on the rights of the child[8], the Commission Recommendation on developing and strengthening integrated child protection systems in the best interests of the child[9], the Digital Education Action Plan (2021-2027)[12], as well as the forthcoming 2030 Roadmap on the future of digital education and skills.

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. The proposal harmonises legislation EU-wide which will support the effectiveness of the EU's external cooperation and global influence in child safety online.

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

• Legal basis

The legal basis for the proposal is Article 114 of the Treaty on the Functioning of the European Union, which provides for the establishment of measures to ensure the functioning of the Internal Market. This proposal aims to approximate rules with the objective to establish the functioning of the Internal Market and, in accordance with article 114(3), ensuring a high level of protection for the health and safety of children across the European Union considering new technological developments.

The main objective of this proposal is to put in place harmonised provisions to protect minors online. As Member States are discussing or adopting new measures to restrict access to certain online platforms considered risky for children under a specified age, the EU market risks becoming increasingly fragmented. This proposal therefore aims to ensure the proper functioning of the internal market, in particular, in relation to the provision of cross-border online social networking services, video-sharing platform services, software application stores, of AI companions and general conversational chatbots, and of online games. Such a harmonised approach also ensures an equally high level of protection for minors across the EU.

Furthermore, this proposal specifies and complements the relevant provisions of Regulation (EU) 2022/2065 as regards the protection of minors, and complements Regulation (EU) 2024/1689 as regards child-specific safety requirements for AI companions and general conversational chatbots. Since both Regulation (EU) 2022/2065 and Regulation (EU) 2024/1689 have Article 114 of the Treaty on the Functioning of the European Union as a legal basis, this proposal follows the same approach.

• Subsidiarity (for non-exclusive competence)

Taking into account that digital services and AI systems are by their nature cross-border, the legislative efforts at national level mentioned above for delayed access of minors hamper the provision of digital services and systems cross-border, create legal uncertainty and obstacles to the implementation of the Single Market, high compliance costs and an unequal level of protection for minors across Europe.

The potential consequences in the absence of immediate action also call for urgent action. Member States are already adopting their own legislation. In 2025 and 2026, several TRIS notifications (Italy, France, Norway, Greece, Poland, Austria, Belgium) were received on age restrictions for certain types of digital services. In almost all other Member States, consultations are ongoing, drafts are discussed in national parliaments or have been announced by governments. National laws differ in terms of scope, age limits and types of restrictions imposed. They propose different definitions or criteria for the types of digital services whose access is to be limited, different ages limits (from 13 to 16 years old), eventually dependent on parental consent. Some of the national legislations under discussion include additional obligations on safety by design. The proliferation of national legislations, with different legal obligations, significantly risks fragmenting the Single Market, reducing legal certainty and increasing compliance costs for providers of digital services while providing an uneven level of protection for minors across the European Union.

Harmonising the rules to protect minors and provide them with a safe online environment should be done at Union level, thereby providing predictability and certainty, reducing compliance costs across Europe and ensuring that all minors, no matter where they live are served by a high level of privacy, safety and security online.

- **Proportionality**

The proposal aims to ensure a strong and coherent framework for the protection of minors online. It does so by introducing an EU-wide access restriction to social media+ for under 13-year-olds. The approach allows for the creation of parental accounts for children between 13 and 15 years. It provides for harmonised access to safe social networking services and video-sharing platforms as of 15 years old, combined with clear safety by design obligations and clear requirements and criteria for the use of age assurance.

The proposal takes the report of the co-chairs of the Special Panel on Child Safety as the starting point, which sets out clearly the risks that minors face online. Against that background, it puts in place a framework that tackles the risks on the services mentioned in the report, without disproportionately impacting fundamental rights (see section below).

Key features of the proposal limit the Regulation to what is strictly necessary to achieve the objectives of the proposal. In particular, the proposal sets out obligations on different types of digital services and systems, depending on the nature of the service or system to ensure that they are targeted and proportionate. This approach addresses the identified problems, while not overburdening providers unconcerned by such problems. The substantive obligations are limited to online social networking services, video-sharing platform services, online games, and providers of software application stores. Following a co-regulatory approach, they build on co-regulatory initiatives for the services in scope of this Regulation, including regarding software application stores and online games. As regards AI systems, the proposal is limited to AI companions and general conversational chatbots that may pose serious risks to health, safety and well-being of minors that are not covered by safety by design requirements specifically aimed to address those risks to minors under Regulation (EU) 2024/1689.

At the same time, small and micro enterprises are not exempted from this Regulation, since they may equally provide harms to minors. It would undermine the objective of this proposal to exclude them from scope.

Exempted from scope because they are unlikely to pose harms to minors are not-for-profit online encyclopaedias, not-for-profit educational and scientific repositories, services and

systems that are designed for purely educational purposes and operated within educational establishments or organisations, open-source software-developing and-sharing platforms, unless the platform itself constitutes an AI system in scope of this Regulation and Regulation (EU) 2024/1689, services and systems specifically developed and operated for the sole purpose of scientific research and development, and services and systems designed, developed and operated by public authorities and for exclusive use of said public authorities or on their behalf.

By establishing a clear framework, accompanied by cooperation between Member States, as well as by co-regulation, this proposal aims to enhance legal certainty, ensure the functioning of the Single Market and increase trust levels.

- **Choice of the instrument**

Article 114 of the Treaty on the Functioning of the European Union gives the legislator the possibility to adopt regulations and directives.

The Commission has decided to put forward a proposal for a Regulation to ensure a consistent level of protection for minors throughout the Union and to prevent divergences hampering the free provision of the relevant services and systems within the internal market. This is necessary to provide legal certainty and transparency for economic operators and children and parents alike.

3. RESULTS OF EX-POST EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

- **Stakeholder consultations**

The proposal directly follows on the recommendations of the co-chairs of the Special Panel on Child Safety Online. As an independent process, the Special panel on child safety online examined risks and opportunities for children on digital services as well as the existing regulatory framework and its gaps. It gathered extensive data and expertise. This independent process brought together experts across the European Union 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' group and children's rights organisations also participated in the meeting. Additional stakeholders provided input throughout the process such as the OHCHR, specialised think-tanks, industry representatives as well as the European Data Protection Board.

Youth was also consulted in preparation of this proposal. The President Youth Advisory Group discussed child safety and wellbeing online in its meeting of December 2026, bringing together the views of children from across all 27 EU Member States. The 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. In December 2025, the Safer Internet Forum, which involved over 200 children, young people and representatives from civil society, industry and national authorities discussed the topic 'Why age matters: Protecting and empowering youth in the digital age'. Better Internet for Kids Youth ambassadors and youth representatives from the child participation platforms were also actively included in the Special panel. Across the groups, youth representatives emphasised the responsibility of digital services in providing safe and age-appropriate services. They highlighted the need for

requirements for safety by design, including age-appropriate defaults settings, recommender systems and interface design.

This consultative process is complemented by the Commission's wider stakeholder engagement in the area of child safety online. This includes consultative processes undertook in the context of the implementation and enforcement of the Digital Services Act as well as the Better Internet for Kids Strategy and its network of Safer Internet Centres and Better Internet for Kids Youth Ambassadors. In the context of the adoption of the guidelines on the protection of minors under Regulation (EU) 2022/2065, a 2024 Call for Evidence, which received more than 170 feedbacks, and a 2025 public consultation, with more than 300 inputs, provided detailed information from a wide range of stakeholders including researchers, civil society, industry and public authorities on good practices and measures on online platforms to design a safe online service for kids. A majority of respondents shared positive view on the measures introduced by the Guidelines, which are largely codified by the present proposal. They also requested additional clarity on the legal nature of the guidelines, and on the situations under which age verification and age estimation are appropriate.

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. The findings show that screen time is a major part of adolescent's daily life, with major risks as nine in ten adolescents have encountered at least one harmful or distressing piece of content online in the past three months, with concerns also regarding interpersonal harms and cyberbullying. 54% of parents and 45% of 13-18 years old consider age delays to be an effective solution and 47% of parents and 48% of adolescents call for better implementation of existing rules by digital services.

Furthermore, the Commission is receiving additional evidence sources on a continuous basis from the European Board for Digital Services and the national Digital Services Coordinators who are responsible for supervising the smaller online platforms and ensuring they provide a safe environment for minors and who closely monitor this area on the ground.

Additional consultative processes where also conducted under related European initiatives, such as the Digital Fairness Act and the Audiovisual Media Services Directive. The consultation and call for evidence on the Digital Fairness Act was opened for 12 weeks on 17 July 2025, collecting extensive feedback from citizens, public authorities and other stakeholders, which collected relevant evidence on addictive design of digital products and deceptive or manipulative interface design, including the impact on such practices on minors. For instance, 5,000 children from the EU Children's Participation Platform were consulted on digital fairness, under the EU Strategy on the rights of the child. Furthermore, on 10 February 2026 the Commission launched a public consultation for the assessment of the Impact of the audiovisual media services directive, 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.

- **Impact assessment**

The most important elements of this proposal build on a rich body of evidence from very different sources, including Impact Assessments informing other, either already adopted or forthcoming, legislative initiatives.

Therefore, the proposed Regulation and its accompanying Staff Working Document ("SWD") on the impacts of the proposal are underpinned by a solid evidence base.

First, the Special panel on Child Online Safety brought together over 60 experts from various fields including health, child psychology and psychiatry, computer and social science, as well as representatives from youth groups, parents' groups and children's rights organisations, and the co-chairs also met with the OHCHR, specialised think-tanks, industry and the European Data Protection Board.

Second, the dedicated analysis of impacts presented in the SWD builds on existing impacts assessments, including for the DSA, Digital Markets Act ("DMA"), AI Act, the proposal for a Regulation to prevent and combat child sexual abuse and the recast Directive on combating the sexual abuse and sexual exploitation of children and child sexual abuse material, as well as the upcoming Digital Fairness Act and the Audio-visual Media Services Directive ("AVMSD").

Third, evidence and data are collected through implementation and enforcement of the DSA, notably 10 preliminary findings in relation to the protection of minors including on addictive design, safe accounts and age assurance, as well as studies, risk assessment reports and stakeholder engagement, in particular during the development of the guidelines on the protection of minors which involved a call for evidence, a public consultation, engagement with children and young people and meetings with the European Board for Digital Services. In this context, engagement with national authorities within the supervisory and enforcement framework of the DSA is ongoing. This provides valuable inputs from investigations and many Member States have conducted inquiries and consultations regarding their national draft laws on the protection of minors, such as Sweden and Germany.

Fourth, international engagement and cooperation further points to sources of evidence by public authorities as well as regulators. The Commission is closely cooperating with other regulators including from Australia and the UK that conduced impact assessments and studies, as well as Brazil and Japan.

Fifth, additional studies include a vast body of academic research, a Eurobarometer on the impact of excessive screen time and social media on young people's mental health conducted in 2026 and a study procured by the Commission on the impacts of age assurance on fundamental rights and its economic costs.

The Commission prepared an accompanying analytical Staff Working Document, including (i) a problem definition, (ii) the explanation of the followed approach, and (iii) an assessment of impacts. The Staff Working Document builds on the report of the co-chairs of the Special panel, as well as evidence and data collected in the context of the Digital Services Act implementation and enforcement, and the preparation of impact assessments, notably for the Digital Fairness Act and the review of the Audiovisual Media Services Directive.

The Staff Working Document outlines the main social and economic impacts of the proposal. In terms of social impacts, the health of minors should be improved as both a direct and indirect impact of the proposal. By delaying access to certain specific services and providing safeguards for age-appropriate digital services, the online environment will become a safer place for minors, limiting the risks they encounter online and their impact on their cognitive development as well as their physical and mental health.

In terms of economic impacts, the marginal costs introduced by this proposal are expected to remain relatively limited with regard to the implementation of most safety by design requirements as these were already present in the Guidelines on the Protection of Minors under article 28 of the Digital Services Act. The requirements to prepare compliance plans and to rely on audits are largely included already in the risk assessments and audit provisions in the Digital Services Act. They also concern providers with a very large user base (45 million monthly active users) which should limit the impact on SMEs since, in principle, they do not reach a scale in their user base equivalent to that of very large online platforms. The implementation of age assurance measures and parental control tools will lead to additional costs for digital services providers. It is not possible to conclusively determine the costs of these adjustments and their incidence, especially for the potentially large number of small and micro providers of online social networking services, video-sharing platform services and video games that were previously not subject to article 28 of the Digital Services Act. However, those costs are mitigated by the development of the EU Age verification solution, the expected increased development of the market for safe design solutions and the fact that similar requirements already exist in EU law and increasingly in third countries. It should also be considered that many digital services providers would likely face many of these costs repeatedly under national legislation, and thus benefit from harmonized rules.

- **Fundamental rights**

The proposal aims at improving, promoting and supporting the respect of the rights of the child online, as enshrined in the Charter of Fundamental Rights of the European Union ("the Charter"). The objective of the access delay is to ensure the comprehensive rights of the child online, including their rights to protection necessary for their wellbeing, health and security, privacy, participation, express their views freely, in line with their age and maturity, taking their best interests as a primary consideration, ensuring their right to development and self-determination free from the risks and harms posed by certain online services and systems. While the services in scope of this Regulation pose significant risks to the health and security of children, they also allow children to express their views freely and to receive and impart ideas, as protected by Article 24(1) and Article 11(1) of the Charter. Therefore, the access delay is strictly limited to account creations on a very defined set of digital services and systems that use certain design features and make available certain functionalities to minors that are proven to be harmful to the health and safety of minors. This measure ensures that this limitation on the child's right to freedom of expression remains proportionate and necessary to meet the objective of general interest as required by the Charter. Access to services that are safe, age-appropriate, designed for children and allow for the appropriate parental control and supervision should not be limited. Additionally, exceptions to the delay are provided to ensure access to information, educational materials and public services.

In line with the UN Committee on the Rights of the Child General comment 25, safety by design requirements are established to ensure the respect of the rights of the child online. Safe settings will provide additional privacy to children, while limited contacts with strangers will diminish risks of cyberbullying and grooming.

Parents and guardians also play an important role in the upbringing and development of their children, as recognised by Article 24(3) of the Charter of Fundamental Rights of the European Union. The respect for private and family life, home and communication is safeguarded by Article 7 of the Charter. Article 14(3) of the Charter ensures that the freedom to found educational establishments with due respect for democratic principles and the right of parents to ensure the education and teaching of their children in conformity with their religious, philosophical and pedagogical convictions shall be respected, in accordance with the national

laws governing the exercise of such freedom and right, while ensuring the respect of other fundamental rights enshrined in the Charter, including Article 21 on non-discrimination and Article 24 on children's rights, taking their best interests as a primary consideration.

In recognition of this important role of parents and guardians, the proposal mandates tools for guardians and provides the possibility for parents to set up accounts in a safe environment for 13-15 years old minors. Those tools must be provided in line with the evolving capacities of children, and in respect with their rights to privacy.

Equally, this Regulation ensures respect of children's rights by strengthening their autonomy. The Regulation 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. The Regulation also allows further control over minors' settings. Furthermore, the proposal helps children in their digital education, literacy and support from parents, caregivers, teachers and educators by providing for Member States to develop national strategies to support the objectives of protecting children online.

Age assurance systems and the requirement to verify the age of users can potentially have important implications for the right to privacy, as well as freedom of expression, participation and non-discrimination of the users. The proposal establishes clear requirements for the deployment and use of age assurance systems as well as safeguards and transitional measures to limit the impact on these fundamental rights to what is strictly necessary to safeguard the health and safety of minors online. 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 and limited to new accounts and existing accounts only when the provider cannot tell with a high degree of confidence that the holder of the account is above the age threshold. By enshrining those criteria in law, the proposal provides for clear legal standards for the use and deployment of age assurance systems ensuring a high standard of data protection for their use. This will promote the deployment of an innovative market of age assurance solutions within the Digital Single Market respectful of fundamental rights.

4. BUDGETARY IMPLICATIONS

It is important that the Commission is sufficiently staffed to carry out the activities under this Regulation. This is especially important because, in exercising its tasks, the Commission will have to supervise some of the financially strongest and technologically most sophisticated companies in the world. Supervising these companies will require staff with highly skilled and specialised profiles. The Commission faces a high political risk if enforcement is under-resourced. Calls for quick action to protect European children online are growing, and making sure that the next generation is effectively protected requires adequate staffing – also to deliver on the fast-track enforcement that will be required by this Regulation.

In order to do so the Commission will rely on the supervisory fee as established in Article 43 of the Digital Services Act. Since this proposal is a specification of the Digital Services Act, its resourcing should equally be based on the same supervisory fee. Further details on the budgetary implications are set out in the LFDS.

5. OTHER ELEMENTS

- **Implementation plans and monitoring, evaluation and reporting arrangements**

The proposal will be rigorously evaluated, notably in terms of the effectiveness of the access delay, the personal scope of the access delay and its proportionality and the safety by design requirements. This evaluation shall account for experience gained in the implementation of the proposal as well as technological, market and legal developments.

This will complement ongoing monitoring under the Digital Services Act.

- **Detailed explanation of the specific provisions of the proposal**

Chapter I sets out general provisions, including the subject matter and scope of the Regulation (Articles 1 and 2) and the definitions of key terms used in the Regulation (Article 3). This sections also sets out anti-circumvention rules for providers in scope of this Regulation (Article 4) and obligations on identified providers to notify and undergo an independent audit of a compliance plan (Article 5).

Chapter II contains provisions on the delayed access of minors to social media, laying down that providers of services that have specific features and that constitute social networking services or video-sharing platforms services, or both, shall not allow minors below the age of 15 to create an autonomous account. Furthermore, providers of those services may allow guardians to set up accounts for minors above the age of 13 with limited age-appropriate features to access the service (Article 6). Where providers of video-sharing platform services can demonstrate that they are an age-appropriate service, they may allow guardians to exceptionally enable, access also to minors below 13 years by means of accounts that are created and supervised by the guardians themselves (Article 7).

Chapter III sets out provisions on safety by design applicable to providers of online social networking services, of video-sharing platform services, of AI companions, of general conversational chatbots and of online games.

Section 1 lays down general provisions applicable to providers of online social networking services, of video-sharing platform services, of AI companions, of general conversational chatbots, of online games, and of software application stores. This section specifies that the requirements laid out in this Chapter also apply to unregistered recipients of the service or users of the system, and that it is only possible to derogate from those requirements when it has been established that the recipient of the service or user of the system is an adult, making use of age assurance in accordance with Chapter V (Article 8).

Section 2 lays down provisions applicable to online social networking services and video-sharing platform services. In particular, those services are prohibited from designing, organising or operate their services in a manner that is intended, or can reasonably be foreseen, to encourage compulsive or excessive use of the service by minors and should put in place effective time-management tools which protects core sleep hours and school time of minors (Article 9). Those providers that use recommender systems are obliged to design the information suggested and the optimisation of their recommender systems to minors in way that ensures a high level of privacy, safety and security of minors (Article 10). Furthermore, those providers shall put in place appropriate and proportionate measures to ensure that settings are set by default to a high level of privacy, security and safety of minors which cannot be changed unless minors have explicitly consented to such changes. Those providers shall ensure that features or settings which have any actual or foreseeable negative effects on

minors' privacy, safety and security are not available to minors (Article 11). Those online social networking services and video-sharing platform services are also obliged to put measures in place that ensure a high level of privacy, safety and security of minors as regards contacts between minors and other recipients of the service (Article 12). Finally, the same providers shall ensure that, before an economic transaction takes place, it is transparent to the minor that this is an economic transaction, and that their still developing commercial literacy is not exploited by design, organisation or operation choices which may lead to excessive, impulsive or unwanted spending, which includes not exposing minors to variable reward systems (Article 13).

Section 3 lays down provisions applicable to AI companions and general conversational chatbots. In particular, this section obliges providers to implement safety by design provisions related to addictive design, safe settings and transparency of commercial transactions set out by Article 9, 11 and 13 of Section 2, as well as specific rules tailored to these systems (Article 14). These rules require providers of AI companions and of general conversational chatbots to put in place strong child-safety protections, including designing the systems so minors are not exposed to features that are likely to create emotional dependencies, preventing harmful interactions, and carrying out testing and post-market monitoring to identify and mitigate harms to minors' safety, health, fundamental rights and well-being and development. 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.

Section 4 lays down provisions applicable to online games. In particular, this section obliges providers to implement safety by design provisions related to addictive design and safe settings set out by Article 9, 11 and 12 of Section 2, as well as specific rules tailored to online games (Article 15). These rules include that online games shall implement safeguards to prevent the online games from being used to entice the minors to initiate contacts on other services which may pose a risk to their privacy, safety and security. Where providers of video gaming platforms allow recipients to create video games the provider shall put in place the necessary software and organisational to allow those video games to comply with the obligations set out in Article 15(1) and (2) and Articles 18 and 20.

Section 5 lays down provisions for age-appropriate access applicable to providers of software application stores. This section obliges those providers to put in place an age-rating system to establish the age-appropriateness of software applications and to assess the age of the recipient of the service through age assurance. Where a software application is not considered age-appropriate, the provider of the software application store shall not allow minors access to such software applications that are age-inappropriate (Article 16). Finally, this section encourages the drawing up of codes of conduct to contribute to the harmonised establishing and application of age-rating systems (Article 17).

Section 6 sets out additional general obligations on agency of minors and empowering tools for minors and guardians applicable to providers of social networking services, of video-sharing platforms services, of AI companions, of general conversational chatbots and of video gaming platforms and games. This section specifies that those providers are obliged to ensure that features, communication, information, user-control tools and mechanisms of the service, warnings, and any other information referred to in Chapter III are easily accessible to all minors and presented in a way that minors can understand. Providers of very large online

platforms within the meaning of Article 33(1) of Regulation (EU) 2022/2065 are obliged to present such information in the in the official language(s) of the Member State(s) the service is provided in. Furthermore, providers of social networking services, of video-sharing platforms services, of AI companions, and of general conversational chatbots**,** and of video gaming platforms are obliged to provide tools enabling minors to control content, their settings and provide to feedback which should have a durable effect on content recommended (Article 18). This section also specifies that those providers are obliged to put in place child-friendly reporting mechanisms and support tools for minors (Article 19) as well as effective, easy to use tools for guardians. Moreover, this section obliges those providers of social networking services, of video-sharing platforms services, of AI companions, and of general conversational chatbots**,** and of online games to encourage the rollout of such tools and requires providers of very large online platform within the meaning of Article 33(1) of Regulation (EU) 2022/2065 to ensure that these tools for guardians are interoperable with tools for guardians provided by third parties, in accordance with conditions set out by Article 6 of Regulation (EU) 2022/1925 (Article 20). Finally, this section sets out that minors and guardians have the right to lodge a complaint with the competent authority against providers of social networking services, of video-sharing platforms services, of AI companions, and of general conversational chatbots**,** and of online games alleging an infringement to this Regulation, minors and guardians have the right to mandate a body, organisation or association to exercise the rights conferred by this Regulation on behalf of the minor or their guardian (Article 21).

Section 7 contains other provisions concerning due diligence for a safe environment online It sets out the monitoring obligations for very large online platforms (Article 22), provisions on drawing up codes of conduct (Article 23), and the obligation for services to have in place legal representatives (Article 24). Finally, it sets out that the Commission is empowered to adopt delegated acts to supplement the measures listed in this Chapter to ensure a high level of privacy, safety and security of minors on their service (Article 25).

Chapter IV contains the obligation to verify parental responsibility (Article 26).

Chapter V contains provisions concerning age assurance.

Section 1 sets out the general principles for age assurance. This section specifies that where providers in scope of Chapters II and III have to implement age assurance solutions, they shall provide a high level of accuracy, reliability, robustness, non-intrusiveness, privacy and non-discrimination, and that self-declaration is not sufficient for compliance with this Regulation (Article 27), it also sets out the specific rules for data protection in age assurance (Article 28).

Section 2 complements this with specific obligations for age assurance, setting out that for the purpose of compliance with Articles 5 and 6, providers should put in place age verification, and for the purpose of compliance with Chapter III they may use both age verification and other age assurance solutions under specific conditions (Article 29), complemented by an empowerment for the Commission to specify details set out in the age assurance Chapter (Article 30). Furthermore, this section requires Member States to take the necessary measures to ensure the availability of different means of obtaining a proof of age attestation to verify the minimum age and to make available at least one age verification solution (Article 31). Finally, this section contains measures on age verification for existing accounts (Article 32).

Chapter VI contains a provision on measures for the Member States to prepare and support minors as this Regulation becomes a reality (Article 33).

Chapter VII contains the provisions concerning the competences, supervision and enforcement of the provisions in this proposal that rely on the existing enforcement structures and frameworks under the Regulation (EU) 2022/2065 and Regulation (EU) 2024/1689 to avoid duplications and ensure consistency with the existing rules for intermediary services and AI systems (Article 34). Where the Commission initiates proceedings for services and systems within its exclusive competence, the Commission shall endeavour to adopt a final decision within 90 days and communicate the preliminary findings to the provider concerned within 30 days from the opening of proceedings (Article 35). Finally, it contains a provision on the financing of supervisory and enforcement activities by the Commission under this Regulation (Article 36) and provisions on the development of expertise and incident reaction mechanisms (Articles 37 and 38).

Chapter VIII contains the provisions on implementing and delegated acts (Articles 39 and 40) and **Chapter IX** contains the final provisions including on the review of the Regulation, inclusion of this Regulation in the Annex of the Representative Actions Directive (Article 41), and the entry into force and application (Articles 42 and 43).

2026/0286 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

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

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee[1],

Having regard to the opinion of the Committee of the Regions[2],

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) Online social networking services, video-sharing platform services, artificial intelligence ('AI') companions, general conversational chatbots, online games, and software application stores that have become an important part of the daily lives of minors. Such information society services and AI systems provide opportunities for minors in the areas of identity development, learning, education, civic participation, relationship development, communication, connection and creativity. At the same time, some of those services and systems, including because of their design, may create risks to minors' privacy, safety and security. These risks include, for example, exposure to illegal or content and risks resulting from cyberbullying or contact from individuals seeking to harm minors. Minors may also face risks as vulnerable consumers through commercial practices that may be manipulative and cause unwanted spending, compulsive and addictive behaviour. These risks can originate from the direct experience of the minor with the online social networking services, video-sharing platform services, AI companions, general conversational chatbots, online games, and software application stores or from the actions of other users on the platform or the systems.

(2) A Special panel of experts on child safety online ('Special Panel') was established to provide advice to the Commission on a European approach on child safety online. The report of the Co-Chairs of the Special Panel was presented in July 2026 and is based on six guiding principles: 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. In particular, the report recommends EU-wide access restrictions to social media, harmonised safety-by-design rules for social media, other digital services, online games and certain AI

[1] OJ C , , p. .
[2] OJ C , , p. .

systems accessible to minors as well as proportionate, privacy-preserving age assurance systems. The intention is to cover the entirety of the digital environment to ensure an effective and comprehensive protection of minors online (social media+).

(3) Member States are increasingly introducing, or are considering introducing, national laws to establish a minimum age for minors to access certain online services. Those diverging national laws negatively affect the internal market, which, pursuant to Article 26 TFEU, comprises an area without internal frontiers in which the free movement of goods and services and freedom of establishment are ensured, taking into account the inherently cross-border nature of the internet and online services and systems. The conditions for providers to restrict minors' access to certain services and systems, as well as obligations regarding the design of their services and systems, require harmonisation so as to create legal certainty for providers offering services and systems accessible to minors across the Union, and ensuring a harmonised level of protection for minors irrespective of their location in the Union.

(4) Regulation (EU) 2022/2065 of the European Parliament and of the Council[3] establishes a horizontal framework of due diligence obligations for providers of intermediary services, including specific obligations concerning the protection of minors online. In particular, Article 28 of that Regulation provides for obligations on providers of online platforms accessible to minors to put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors, on their service. The Commission Guidelines on measures to ensure a high level of privacy, safety and security for minors online[4] set out a non-exhaustive list of measures that providers of online platforms accessible to minors should put in place to comply with their obligation under Article 28(1) of Regulation (EU) 2022/2065.

(5) This Regulation specifies and complements the relevant provisions of Regulation (EU) 2022/2065 as regards the protection of minors, in particular in order to ensure a high level of privacy, safety, and security of minors, taking into account the Guidelines and the report drawn up by the co-chairs of the Special Panel. To that end, this Regulation sets out rules for a harmonised minimum age for creating an account with online social networking services, video-sharing platform services, and rules for harmonised design requirements for such services, and for age assurance.

(6) For that purpose, the provisions laying down a harmonised minimum age for creating an account with online social networking services and video-sharing platform services, harmonised safety requirements for online social networking services, video sharing platform services, video gaming platform services and software application stores, and harmonised rules regarding age assurance online and parental responsibility, insofar as they operationalise the obligation to put in place a high level of privacy, safety and security of minors, specify Article 28 of Regulation (EU) 2022/2065.

(7) Nothing in this Regulation should be construed as an imposition of a general monitoring obligation or a general active fact-finding obligation, or as a general obligation for providers of intermediary services to take proactive measures in relation to illegal content.

---

[3] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (OJ L 277, 27.10.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2065/oj).

[4] 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 (OJ C, C/2025/5519, 10.10.2025, ELI: http://data.europa.eu/eli/C/2025/5519/oj).

(8) This Regulation also complements Regulation (EU) 2024/1689 of the European Parliament and of the Council[5], which sets out a comprehensive, risk-based framework for the regulation of AI in the Union. Regulation (EU) 2024/1689 prohibits certain AI practices, including harmful exploitation of minors' vulnerabilities and manipulation. Furthermore, it lays down requirements for high-risk AI systems, transparency requirements for interactive and generative AI systems and obligations for providers of the most capable general-purpose AI models to assess and mitigate systemic risks, including risks to the safety and well-being of minors. Without prejudice to the requirements and obligations set out in Regulation (EU) 2024/1689, this Regulation aims to address the particular risks posed to minors by AI companions and general conversational chatbots and to specify harmonised measures that providers of those AI systems should adopt to ensure a high level of protection of minors' health and safety and to support their physical, mental and emotional well-being and development.

(9) This Regulation should be seen as part of the EU overall efforts to protect users, including children and other vulnerable groups, from being exposed to illegal content online. This includes Directive (EU) 2024/1385 on combating violence against women and domestic violence, which criminalises the non-consensual sharing of intimate images or manipulated material, gender-based hate speech, cyber harassment, and cyber stalking, including where directed at minors.

(10) This Regulation is without prejudice to the rules laid down in Directive 2010/13/EU regulating other aspects of the provision of these services covered by this Regulation, in particular, rules on the protection of minors as viewers of the audiovisual content. Where other instruments of Union law regulate similar, but not more specific, aspects of the provision of services in scope of this Regulation, the latter should prevail.

(11) Building upon definitions covering the digital environment, this Regulation should apply to certain information society services as defined in Directive (EU) 2015/1535 of the European Parliament and of the Council, that is, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient. Specifically, this Regulation should apply to providers of online social networking services and of video-sharing platform services. This Regulation should also apply to certain AI systems within the meaning of Article 3(1) of Regulation (EU) 2024/1689 that are accessible to minors and that qualify as AI companions or general conversational chatbots. In addition, this Regulation should apply to providers of operating systems as defined in Regulation (EU) 2022/1925, as well as to providers of software application stores as defined in Regulation 2022/1925, which is a type of online intermediation service focused on software applications as the intermediated product or service. For the avoidance of doubt, this Regulation applies also to those online social networking services, video-sharing platforms, and software application stores that are designated as very large online platforms pursuant to Article 33 of Regulation (EU) 2022/2065.

(12) Video games have become an important part of the digital environment in which minors participate and interact with others, in a playful, goal-oriented or entertaining manner. Certain video gaming platforms allow the dissemination and exchange of user-generated content to an indeterminate number of recipients of the service and the

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

facilitation of contact between these recipients. Such online games fall within the definition of online platforms referred to in Regulation (EU) 2022/2065 and should be covered by the scope of this Regulation. At the same time, some online games that do not allow the dissemination of information to an indeterminate number of recipients should also fall within the scope of this Regulation. This is the case of any game that that can be played on a computer, a mobile device, or a games console, irrespective of whether the game underlying software is subsequently executed locally, remotely, such as by means of durable medium, and irrespective of whether the service is provided free of charge, against payment, or against hybrid remuneration involving in-service (or in-application) purchases. Online games that are accessible or purchasable exclusively through physical media, without any online component enabling their access, distribution, or purchase, are not considered online games for the purposes of this Regulation. For the avoidance of doubt, where an online game also has certain features corresponding to a video sharing platform, it shall be considered an online game for the purpose of this Regulation.

(13) To ensure proportionality of the Regulation, this Regulation should not apply to services or systems that, by virtue of their non-commercial, educational, scientific or public-interest nature, present a materially very low risk to minors. This exclusion should cover not-for-profit online encyclopaedias, not-for-profit educational and scientific repositories, services and systems that are designed for primarily educational purposes and operated by educational establishments or organisation, or for them; open-source software-developing and-sharing platforms, services and systems specifically developed and operated for the sole purpose of scientific research and development, and services and systems designed, developed and operated by public authorities and for exclusive use of said public authorities or on their behalf.

(14) Where providers of services falling within the scope of this Regulation are also subject to the obligation to ensure a high level of privacy, safety and security pursuant to Article 28(1) of Regulation (EU) 2022/2065, these obligations are specified for the subject matters covered in this Regulation. Compliance with the obligations set out in this Regulation should however not be construed sufficient in itself to constitute proof of compliance of such providers with Article 28(1) of Regulation 2022/2065 and should therefore be without prejudice to further mitigation measures which such providers may be required to put in place for matters not covered by this Regulation for example those related to ensuring security. Equally, Article 28(1) of Regulation (EU) 2022/2065 should remain applicable to online platforms outside of the scope of this Regulation.

(15) For the purposes of this Regulation, it is appropriate to establish a common definition of a minor or child. A 'minor' or 'child' should be understood as any natural person under the age of 18, irrespective of any provisions of national law providing for an earlier or later attainment of legal majority. Furthermore, while providers of online social networking services, of video-sharing platform services, online games, software application stores and AI systems remain primarily responsible for the safety of their services and systems when used by minors, parents and legal guardians can play a role in guiding the minors' experience online. The notion of guardian for the purpose of

this Regulation should be based on the definition of parental responsibility in Council Regulation (EU) 2019/1111[6].

(16) For the purposes of this Regulation, the definition of 'AI system' as defined in Article 3, point (1), of Regulation (EU) 2024/1689 should apply. It is furthermore appropriate to define certain types of AI systems that qualify as AI companions or general conversational chatbots and are subject to the complementary obligations under this Regulation. Where reference is made to a provider of an AI companion or of a general conversational chatbot in this Regulation, the notion of provider should be understood as defined in Article (3), point (3), of Regulation (EU) 2024/1689.

(17) The definitions relating to age assurance, including 'age verification', 'age assurance', 'EU list of providers of EU proof of age attestations', EU list of providers of EU Age Verification Solutions', 'EU Age Verification Scheme' and 'proof of age attestation', should be understood as building on, and being interpreted consistently with, the Union framework established by Regulation (EU) No 910/2014 of the European Parliament and of the Council as amended by Regulation (EU) 2024/1183, as well as with Commission Recommendation (EU) 2026/1035 of 29 April 2026 on establishing a common framework for EU wide Age Verification technologies for minors and the related Commission Guidelines on the protection of minors online.

(18) To ensure that a high level of privacy, safety and security for minors is guaranteed, it is important that the obligations are applied effectively and are not circumvented. Accordingly, providers should not engage in behaviour that would undermine the effectiveness of the obligations laid down in this Regulation. Such behaviour includes the design of the service or the system, the presentation of choices to recipients of the service or user of the system in a non-neutral manner, or using the structure, function or manner of operation of a user interface or a part thereof to subvert or impair user autonomy, decision-making, or choice. For example, minors should not be requested to lower the level of sensitive settings during account creation, such as access to geolocation or camera. They should also not be enticed to circumvent the delayed access obligations. Providers should also limit the creation, by minors, of secondary accounts aimed at circumventing safety by design measures.

(19) To ensure that services that minors are accessing provide for the highest level of privacy, safety and security, the providers of online social networking services and video-sharing platforms services that have been designated as very large online platforms designated pursuant to Article 33 of Regulation (EU) 2022/2065 should notify to the Commission of measures they intend to take to ensure effective compliance with the obligations, such as delayed access to service and safety-by-design. This should enable the Commission to verify, following an assessment by independent auditors with a specific expertise that the providers subject to the obligations laid down in Chapters II to V of this Regulation have taken the measures necessary to comply with them. The Commission should respond to that compliance plan, without prejudice to its supervisory and enforcement powers, in particular the power to initiate proceedings pursuant to Article 34 of this Regulation. This notification mechanism is necessary and proportionate in view of the objective it pursues and respects fundamental rights of freedom to conduct a business enshrined in

[6] Council Regulation (EU) 2019/1111 of 25 June 2019 on jurisdiction, the recognition and enforcement of decisions in matrimonial matters and the matters of parental responsibility, and on international child abduction (OJ L 178, 2.7.2019, p. 1, ELI: http://data.europa.eu/eli/reg/2019/1111/oj).

Article 16 of the Charter and with the freedom to receive and impart information under Article 11 thereof.

(20) The years from 0 to 15 are particularly important for minors' cognitive, emotional and social developments, as well as for the development of their personality, identity and value systems. Scientific evidence shows that certain online social networking services and video-sharing platform services pose a particularly serious risk to the privacy, safety and security of minors below the age of 15 years due to their particular features and functionalities. Ranging from risks as passive online users under the age of 3, when care can be substituted by screentime 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, to risks of convergence of developmental sensitivities and platform-driven amplification of content and interactions, research shows mental health impacts and that children are especially vulnerable under the age of 13. Until 15, adolescents transition into autonomy, and whilst supervision by caregivers and educators becomes less effective, risks are increasingly shaped by social elements of digital services, rather than individual behaviours, and adolescents from 13 to 15 are at the peak of developmental vulnerability. It is therefore crucial to ensure that their right to development and self-determination can be enjoyed free from the substantial impacts that the risks and harms posed by certain online services can have on minors. In order to ensure an equal level of protection for minors located in the Union, introducing an EU-wide access restriction to social media+ for under 13-year-olds is necessary. In order to avoid fragmentation of the internal market by diverging national laws, a harmonised minimum age of 15 years should be established for creating autonomous accounts with online social networking services and video-sharing platform services that present features or functionalities that are particularly harmful for minors below that age. This should be without prejudice to Union laws or national laws in accordance with Union law, establishing a higher minimum age for specific categories of content such as pornographic or gambling content.

(21) The features and functionalities which are considered to pose a risk to the privacy, safety and security of minors below the age of 15 correspond to globally recognised classifications of online risks, including exposure of minors to age-inappropriate content or contacts as well as harmful conducts of other users or other commercial or cross-cutting risks such as excessive use. These therefore include features and functionalities that enable certain harmful content consumption and dissemination as well as harmful interactions or behaviour. In particular, services enabling recipients to disseminate content in real-time to an indeterminate number of people expose minors to risks for their privacy as well as to inappropriate content, such as pornographic content; enabling minors to interact with unknown users exposes them to risks of inappropriate contact by adults but also of abusive or other harmful conducts by other users; automatically suggesting content or contacts expose minors to the risk of being exposed to harmful content or so-called "rabbit-holes" of harmful content, as well as entering into potentially harmful contacts with malicious users; deploying functionalities, interface designs or characteristics that can lead to compulsive or excessive use, such as push notifications or endless content feeds, expose the minor to risks of developing behaviours that harm their mental health and wellbeing, including addictive behaviours. These functionalities are typically offered only to recipients of the service that access the service by means of an account. It is therefore proportionate, taking into account the minor's right to freedom of expression, to delay

access to the service at the point of creation and use of such accounts, as the use of the same service without an account poses a lower risk to minors.

(22) Recognising the role of parents and legal guardians in supporting the evolving autonomous and safe development of minors online, it is appropriate to allow providers to exceptionally derogate from the minimum age for autonomous access laid down in this Regulation, down to a lower minimum age of 13 years, to allow the holder of parental responsibility to set up an account with limited functionalities for children between 13 and 15. Such an account should be an account of the holder of the parental responsibility and not of the respective minor. That derogation should be subject to verification of parental responsibility and should not undermine the objective pursued by this Regulation, taking into account the children's right to protection, privacy and taking the child's best interests as a primary consideration. Finally, that derogation should not be possible where the providers in their terms of service restrict access to and use of their service for users below a higher minimum age than 13 years.

(23) Where a video-sharing platform service is specifically designed for minors below the age of 13 years, a guardian may exceptionally enable such a minor to access the service under the conditions laid down in Article 7, exclusively through the guardian's own account and under the guardian's control and supervision. Such guardian-controlled access does not entail the creation or use of an account by the minor and is therefore not access by means of an account created for, or attributed to, the minor within the meaning of Article 6(1). Guardian-controlled access may be organised through child-specific settings or profiles within the guardian's account; such settings or profiles do not constitute accounts of the minor.

(24) Nothing in this Regulation requires any provider to make its service available to minors below the age of 13, nor does it affect the terms and conditions of services that exclude such minors, which remain fully subject to the obligations of this Regulation to prevent their access. Requirements related to the age-appropriate experience on video-sharing platforms services concern solely those services whose providers have made the deliberate choice to offer an environment specifically designed for children, and subjects that choice to strict conditions.

(25) Age-appropriate and safe online experiences are paramount to protect minors in an increasingly online environment. In order to ensure that minors can benefit from a safe digital environment, providers of online social networking services, video-sharing platform services, online games, AI companions, general conversational chatbots, and software application stores, should put in place appropriate and proportionate measures to ensure a high level of privacy, safety and security of minors when using their service or system. To that end, providers should by-design shape their services and systems in a way that prioritises the wellbeing of minors by embedding privacy, safety and security protections into their design and operation from the start taking into account the evolving capacities of minors. Where the service or system is accessible without registration or authentication, providers should by default configure the design and settings for any unregistered or unauthenticated user in a way which guarantees a high level of privacy, safety and security of minors. Providers should only derogate from those requirements once they have established that the recipient or user is an adult by making use of age assurance in accordance with this Regulation.

(26) For online social networking services and video-sharing platform services, the measures taken by providers of those services to comply with the obligations set out in

this Regulation should ensure that, once minors have created their own account to use the service, they continue to benefit from a safe digital environment. While those measures mitigate the risks arising from the particular functionalities and features of such services for minors above the age of 15 years, online social network services and video sharing platforms nevertheless remain inappropriate for minors below that age. Compliance with those obligations should therefore not affect the general restriction on minors creating their own account below that age.

(27) Certain design features of online social networking services and of video-sharing platform services may exploit minors' vulnerabilities and contribute to extensive or excessive use of the service, compulsive behavioural patterns or addiction-like behaviour, with adverse effects on minors' mental, emotional and physical well-being. Such features may include uninterrupted content consumption without effective stopping points, autoplay, autoscroll, autoreplay, infinite scroll, notifications artificially timed to regain attention, reward mechanisms encouraging repeated engagement, or mechanisms penalising the recipient of the service for not returning at regular intervals. Providers of online social networking services and video-sharing platform services should therefore not expose minors to manipulative or persuasive design features predominantly aimed at maximising engagement where those features may impair minors' privacy, safety or security or undermine their autonomy. Providers of online social networking services and of video-sharing platform services should not undermine the minor's decision to discontinue use or the absence of decision to use the service, such as notifications not triggered by, or not directly related to, the minor's interaction or activity on the service. This should cover situations where the platform changes behaviour towards users when users do not use the service. As such, this would cover features which attempt to recapture user attention once lost, such as sending notifications about rewards for continuing to use the service. The providers should also not incentivise engagement at regular times or with greater frequency, including through penalties or loss of benefits for failing to engage regularly or within specified time intervals. The providers should implement age-appropriate time-management and agency-enhancing tools, including visible prompts, reminders and other measures that support informed and deliberate use of the service enabling effective interruption of the use of the service. As time-management tools are often overridden by the minors themselves, providers should ensure these measures are effective in reducing minors use of the service and not easily circumvented. Such tools should also ensure that minors' sleep needs are not impaired by their use of the service. That should include effectively preventing minors from using the service during their school time and core sleep hours, which should be age-appropriate, in accordance with scientific recommendations. Core sleep hours should be understood as the period of the night during which minors are ordinarily expected to sleep, comprising at least eight consecutive hours between 22:00 and 08:00 local time. School time should be understood as the period during which minors are ordinarily expected to attend school or otherwise participate in compulsory educational activities, in accordance with applicable national law or practice and subject to adjustment by guardians.

(28) A core aspect of the design and operation of online social networking services and of video-sharing platform services is the manner in which information is prioritised and presented on the service's online interface, which may significantly influence minors' access to, engagement with and exposure to information. To ensure that minors are effectively protected online, providers of online social networking services and of video-sharing platform services that use recommender systems should design their

recommender systems in such a way that they ensure a high level of privacy, safety and security of minors. To that end, providers should use evaluation metrics that capture quality, safety and mental-health outcomes for minors, such as metrics measuring whether the recommender system selects and prioritises content appropriate for a minor's age and developmental stage, assessing the system's effectiveness in preventing exposure to illegal, harmful or unsafe material, and capturing indicators of psychological well-being to assess the impact on minors' mental health. Those metrics should inform the optimisation considerations underlying the design of recommendation objectives of online platforms. To ensure a high level of privacy, safety and security of minors, providers of online social networking services and of video-sharing platform services should give priority and primary weight to explicit user-provided preferences when recommending content, such as user feedback and interactions that indicate users' explicit preferences, both positive and negative, including the stated and deliberate selection of topics of interest, surveys, reporting, and other quality-based signals. Furthermore, to ensure minors are provided with more agency over information being suggested to them, providers of online social networking services and of video-sharing platform services should disable by default the recommendation of information suggested by the recommender system based on implicit engagement-based signals from minors' behaviour online. Implicit engagement-based signals should be understood as signals and data that infer user preferences from their activities (browsing behaviour on a platform), such as time spent viewing content and click-through rates. Providers of online social networking services and of video-sharing platform services should ensure that recommender systems do not rely on the collection of any personal data captured from outside the service. Providers of online social networking services and of video-sharing platform services should also ensure that minors are not exposed to content that is harmful when encountered repeatedly, which should be understood as covering the so called "rabbit holes" or "filter bubbles" of content that may pose a risk to their safety and security. The "rabbit hole" effect relate to the progressive amplification of similar recommendations of content, leading recipients of the service to endless content pathways which could potentially be extreme and harmful to minors. The "filter bubble" effect refers to the progressive amplification of content whereby a minor is predominantly exposed to content or information reducing the minors' exposure to diverse content or information. Minors should also be given agency over their recommender systems and be able to control the content recommended through dedicated tools. Minors should be offered an easy way to reset their recommender systems by deleting all previous identified preferences and, be able to choose one option that is not based on profiling irrespective of whether they are registered or not, as provided for in Article 38 of Regulation (EU) 2022/2065, regardless of whether or not the provider concerned is a provider of a very large online platform in accordance with Article 33 of Regulation (EU) 2022/2065. To ensure the effectiveness of such measure, those providers should regularly remind minors of the option to reset their feeds and ensure that that option is not designed in a manner to entice minors into choosing the option based on profiling.

(29) Designing settings to ensure a high level of privacy, safety and security is important to minimise online risks for minors by reducing the likelihood of minors being exposed to content, interactions or functionalities that may be harmful, including in circumstances where children are unregistered on the service. To this end, providers of online social networking services and of video-sharing platform services should ensure that settings, such as those that allow tracking recipients of the service or locating

them, enabling access to microphone, contacts and camera, or recommending other accounts to minors are off by default for minors. When enabled, some particularly privacy-sensitive settings, such as access to location, should be turned off after the session ends, and in any case, minors should always be made aware when activated. Furthermore, push notifications should be turned off by default and should be designed in a way that does not impair minors sleep needs and school time. To this end, push notifications should never be sent to children during their school time and core sleep hours, with the exception of where such notifications stem from urgent security alerts – for example related to account security - or interactions with their guardians. Push notifications are notifications that appear on a device to inform the recipient of the service of ongoing activities on the service regardless of whether the service is actively in use and thereby encouraging users to continue the use of the service. Additionally, where some settings and features may be particularly harmful to minors, providers should make them inaccessible for minors. Such harmful features can be filters impairing minors' mental well-being for example by disproportionately embellishing, distorting or idealizing a child's image – excluding harmless filters such as those mimicking animals – as well as features increasing social comparison such enabling children to see the numbers of reactions on their content.

(30) Minors should be protected from contact-related risks, including cyberbullying, harassment, and those seeking to groom, sexually abuse or extort minors, human traffickers and those seeking to recruit minors into criminal gangs or promote violence, radicalisation, violent extremism and terrorism, as perpetrators often use the digital space to reach out to children. Consequently, interactions between minors and unregistered recipients of the service, as well as unknown recipients of service, especially adults, should have robust safeguards. Providers of online social networking services and video-sharing platform services should ensure that information about the minor, such as profile information, biography, activities, list of friends, followers and similar information cannot be accessed by recipients of the service by default, and in any event, by recipients of the service without accounts. Minors should be empowered to exercise effective control over the visibility of their personal information, such as their profile photo, profile information, content shared, contacts, activities and history or any other data shared on the account or profile. Contact details from minors – including but not limited to address, email address and telephone number – should not be shared with other recipients of the service. Minors should be able to block any other recipient of the service, manage content shared and regulate the interaction and related metrics, such as likes and number of followers. By default, the hosting of livestreams or other real-time transmissions should be disabled, as should access to the minor's account information by recipients of the service who have not been explicitly accepted. To ensure that the possibility to enable these settings remains proportionate, this should depend on the age and evolving capacities of the minor, for example by ensuring that public accounts and the possibility to host livestream should only be accessible to children above the minimum age and if explicitly consented by their guardian.

(31) Commercial practices occur in different forms on digital services and can have particular persuasive effects on minors, who face diverse, dynamic and personalised tactics, through for example, advertisements, product placements, the use of virtual currencies, influencer marketing, sponsorship or AI-enhanced nudging. In line with, and without prejudice to, the existing horizontal legal framework, in particular the

Directive 2005/29/EC of the European Parliament and of the Council[7] that is fully applicable to all commercial practices including towards minors as consumers and the rules in Regulation (EU) 2022/2065 on advertising (Article 26, Article 28(2) and Article 39) and dark patterns (Article 25). In the particular case of dark patterns, Regulation (EU) 2022/2065 acts as the "safety net" complementing Directive 2005/29/EC. Economic transactions may be harmful to minors' safety and security when using the service, especially where they do not understand the consequences of the transaction they are making. Therefore, minors should be clearly informed about economic transactions taking place online. To this end, purchases carried out within the service should be labelled as an economic transaction in an easy comprehensible manner and in real time. Virtual currencies and other tokens may also cause unwanted spending, therefore all kind of purchases should be displayed in the national currency of the habitual residence of the minor. Moreover, providers of online social networking services and of video-sharing platform services should ensure that minors as vulnerable consumers are not exploited and should not design their platform in such a way that can lead to excessive, impulsive or unwanted spending. This should include notably introducing a separation or friction between content and the purchasing of related products as well as preventing minors from being exposed to loot boxes and other products, where they offer random or unpredictable outcomes or gambling-like features.

(32) Given the particular vulnerabilities of minors and the risks that AI companions and general conversational chatbots may pose to their health, safety, fundamental rights and well-being, providers of such AI systems should implement safety by design measures tailored to the specific characteristics and risks stemming from those systems in order to offer minors an age-appropriate experience. Safeguards should include safe settings and prohibitions on addictive designs. Furthermore, minors should not be exposed to features of the system displaying behaviours or simulating emotions or interpersonal relationships that are likely to create emotional and other dependencies, including when such dependencies may negatively impact relationships with other humans and the development of the minor. In order to prevent such systems from accumulating sensitive data of minors and potentially reinforce harmful interaction patterns over time, the persistent conversational memory of interactions with minors should be disabled by default except where necessary to protect their safety. AI companions and general conversational chatbots accessible to minors should also be subject to appropriate testing and evaluation before being placed on the market or put into service and at regular intervals thereafter.

(33) Providers of AI companions and of general conversational chatbots accessible to minors should also implement post-market monitoring to identify and mitigate risks to minors' health, safety and fundamental rights and their mental, physical, mental and emotional well-being and development and to assess the effectiveness of the measures put in place, unless the provider is a micro or small enterprise. In this context, it should be borne in mind that if the AI companion or general conversational chatbot is based on a general-purpose AI model with systemic risk, that models is already subject to specific risk management obligations under Regulation (EU) 2024/1689. The

[7] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, 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, p. 22, ELI: http://data.europa.eu/eli/dir/2005/29/oj).

systemic risk management carried out by providers of those models should include the assessment, and, if necessary, mitigation of risks to the safety and well-being of minors, including risks to minors from their legitimate use of the model and from the use of the model by other persons that may cause harm to minors. It is accordingly appropriate for relevant mitigations implemented as part of this systemic risk management pursuant to Article 55 of Regulation (EU)2024/1689 to be relied upon by providers of AI companions and general conversational chatbots as part of their efforts to comply with the requirements of this Regulation. Similarly, risk assessments and mitigation measures implemented pursuant to Articles 34 and 35 of Regulation (EU) 2022/2065 may also be taken into account when performed by a provider of an AI companion or a general conversational chatbot deployed as a functionality of an online social networking service or of a video-sharing platform service in the provision of that service. Nevertheless, such mitigation measures should not be considered sufficient for compliance with the requirements set out in this Regulation.

(34) Where an AI companion or a general conversational chatbot is deployed as a functionality of an online platform or of an online search engine, the obligations laid down in Regulation (EU) 2022/2065 should continue to apply to the provider of those intermediary services, where the conditions for their application are fulfilled. In particular, the deployment of such functionalities should not affect the application of the rules on the assessment and mitigation of systemic risks, including risks stemming from the design, functioning or use of those functionalities, insofar as they form part of the service offered by the online platform or online search engine. To ensure transparency over interactions with such systems, providers of online social networking services, of video-sharing platform services, and of online games that deploy AI companions or general conversational chatbots as a functionality in the provision of their service should also implement measures that empower minors to make informed choices whether to use those companions or chatbots and be able to opt out from such use. This should include obligations for those providers to ensure that minors are not nudged to use those systems through design techniques, such as displaying AI companions and general conversational chatbots at the top of the minor's contacts list. Moreover, safeguards should apply to AI companions and general conversational chatbots when they are deployed as a functionality in the provision of an online game, where in-game purchases can occur.

(35) Online games can take very different forms and can be divided into categories such as action, adventure, role-playing games, strategy, sports, simulation or puzzle games and are usually played on a PC, mobile device or console. Online games can provide minors not only entertainment, but also online environments for communication and social interaction, including for minors with disabilities. Multiplayer online games enable minors to engage with other persons and to build social connections across different age groups and geographical locations. Online games can also contribute to minor´s learning of coordination, cooperation and subjects such as science, mathematics and languages. Video gaming platforms enable users to play and create their own content or games, and disseminate them to the public. Both video games and video gaming platforms may present diverse risks to minors. This was also highlighted by the Report by the Co-Chairs of the Special Panel on Child Safety Online which highlighted that video games may expose children to harmful commercial practices or dangerous contacts and age classification systems may provide orientation and insights for parents and caregivers on game ratings.

(36) Given the particular vulnerabilities of minors and the risks that online games may pose to their privacy, safety and security, it is important that providers of online games implement safety by design measures tailored to the specific characteristics and risks stemming from those online games in order to offer minors an age-appropriate experience. Such risks relate in particular to unsolicited communication in the video games, age-inappropriate content, and design mechanisms which can lead to addictive behaviours and excessive use. Online games with open communication expose minors to contact-related risks, including cyberbullying, harassment, and those seeking to groom, sexually abuse or extort minors, human traffickers and those seeking to recruit minors into criminal gangs or promote violence, radicalisation, violent extremism and terrorism, as perpetrators often use the digital space to reach out to children. Similarly certain settings may expose minors to content, interactions or functionalities that may be harmful, including in circumstances where children are unregistered on the service. Providers of online games should therefore implement safeguards to prevent the service from being used to entice minors to initiate contacts on other services which may pose a risk to their privacy, safety and security. This could be done through restricting link-outs where this may pose a risk to minors and by implementing warning messages to minors. Video gaming platforms may also increase the risk of minors being exposed to age-inappropriate content. Where video gaming platforms allow recipients of the service to create individual video games, the provider of the video gaming platform should put in place the necessary software and organisational measures to allow the provider of the newly created video game to comply with applicable rules.

(37) Certain design features of online games may exploit minors' vulnerabilities and contribute to extensive or excessive use of the service, compulsive behavioural patterns or addiction-like behaviour, with adverse effects on minors' mental, emotional and physical well-being. Online games should therefore not expose minors to features undermining the minor's decision to discontinue use or the absence of decision to play the online game or features or rewards incentivising engagement at regular times or with greater frequency, including through penalties or loss of benefits for failing to engage regularly or within specified time intervals.

(38) Providers of software application stores are in a unique position concerning the way how services which pose a risk for minors may be offered recipients. To ensure a high level of privacy, safety and security for minors in the online environment, providers of software application stores should put in place an age rating system to allow to establish the age-appropriateness of software applications disseminated through their service. Such an age-rating system should apply to each software application and should take due account of the rights and best interests of the child, including minors' evolving capacities and differing levels of maturity. Providers of software application stores should prevent minors from accessing or purchasing applications rated as age-inappropriate. Furthermore, to ensure compliance with applicable Union law and national law adopted in compliance with Union law, where the provider of a software application store becomes aware of software applications disseminated through its service that are or primarily consist of content that is subject to a higher minimum age under the applicable Union law or national law, the provider should not allow minors below that minimum age from that Member State to access or purchase those software applications through its service. For this purpose, providers of software application stores should assess the age of the recipient of the service in accordance with Chapter V of this Regulation. To ensure transparency and accountability, providers of software application stores should make publicly available, in clear and accessible terms,

information on the methodology, criteria and sources underpinning their age-rating systems.

(39) Codes of conduct can be an important tool to protect minors in the online environment. In that context, the Commission should encourage the drawing up or further development of voluntary codes of conduct at Union level establishing common methodologies and criteria for age rating systems, to contribute to the harmonised operation of such systems in the application of this Regulation, including by providers of software application stores. The codes of conduct should in particular facilitate the mutual recognition and consistent application of age ratings across Member States, define appropriate criteria, methodologies and sources of information for assessing the age-appropriateness of the most relevant types of content including violent, sexual, gambling and self-harm content as well as in-app purchases, contact risks and addictive design features as well as establish the necessary remedies and redress mechanisms and ensure transparency, combined with regular, transparent and independent monitoring and evaluation of the achievement of the objectives aimed at. The refusal without proper explanations by a service provider of the Commission's invitation to participate in the application of such a code of conduct could be taken into account, where relevant, when determining whether the service provider has infringed the obligations laid down by this Regulation. The mere fact of participating in and implementing a given code of conduct should not in itself presume compliance with this Regulation. The Pan-European system (PEGI) age classification system and PEGI Code of Conduct set a benchmark for the participating companies with respect to age labelling, promotion and marketing and reflects the video games industry's commitment to provide information to the public in a responsible manner. The rules on codes of conduct under this Regulation could serve as a basis for already established co-regulatory efforts at the Union level to be integrated as a code of conduct. This includes, but does not concern exclusively, the PEGI age rating system, provided that it provides a high level of privacy, safety and security of minors as required by this Regulation.

(40) Minors playing online games should benefit from the same protection in respect of economic transactions as on online social networking services and video-sharing services, including transparency as to the real monetary value of transactions carried out through virtual currencies and protection from exposure to variable reward systems, whose association with gambling-related and compulsive behaviours is well documented. Codes of conduct in the area of online games should build on existing pan-European classification and self-regulatory frameworks or age classification systems at Member State level, including their recent extension to interactive risk categories and monetisation practices, and should keep such frameworks updated in light of scientific and technological developments and emerging risks to minors. Adherence to a code of conduct assessed as adequate by the Commission may serve as an indication of compliance with the measure-based obligations laid down in this Regulation, but cannot derogate from its prohibitions.

(41) In order to ensure a high level of privacy, safety and security of minors in the digital environment, providers of online social networking services, of video-sharing platform services, of AI companions and of general conversational chatbots and of online games should take into account the evolving capacities, interests and vulnerabilities of children throughout the design, development and operation of their service. The measures put in place should therefore at least be child-friendly, easy-to-understand, easily accessible to all minors, including those with disabilities or additional

accessibility needs. Very large online platforms within the meaning of Article 33 of Regulation (EU) 2022/2065 shall ensure that such information is presented in the official language(s) of the Member States in which the service is provided. Providers of online social networking services, of video-sharing platform services, of AI companions and of general conversational chatbots and of online games should also enable minors to provide feedback on content, search results and prompts recommended to them on the service. Such feedback should be taken into account and have an imminent and durable impact on children's experience on the service. Furthermore, minors should be progressively empowered to understand and manage their default settings. Where a minor changes a protective setting, providers should present clear warnings and offer easy reversibility, including the option to temporarily change the setting and one-click return to default settings. In order to ensure a high level of privacy, safety and security of minors, providers should not repeatedly prompt or entice minors to lower their level of protection.

(42) In order to ensure a high level of privacy, safety and security of minors, it is necessary to put in place effective, visible and child-friendly mechanisms for reporting and for supporting minors to report content, accounts, groups, features and behaviour that may negatively affect their privacy safety and security when using the service. This includes the reporting of accounts owned by users below the minimum age, pursuant to this Regulation. Such mechanisms should not affect the application of Article 16 of Regulation (EU) 2022/2065. In order to ensure a high level of privacy, safety and security of minors, such mechanisms should, where appropriate, enable minors to submit a report in their own words and should ensure that the identity of the minor remains confidential towards other recipients of the service or users of the system by default. Reports submitted by minors should be treated as a matter of priority. Furthermore, minors should receive a confirmation of receipt, together with age-appropriate information on the follow-up process, indicative timelines and possible outcomes. Any restrictions imposed by providers following such reports by minors should be considered as a restriction of the visibility pursuant to Article 17(1), point (a) of Regulation (EU) 2022/2065, where applicable. Additionally, minors should be able to access comprehensive and appropriate support where they encounter illegal and harmful content and activities. To that end, providers of online social networking services, of video-sharing platform services, of AI companions and of general conversational chatbots, and of video gaming platforms services, should make available support tools that are easily accessible and adapted to the needs of minors and that enable referrals or connection to national support services, including Safer Internet Centres, child help and hot lines, child protection services and, where appropriate, contact details of law enforcement. Those support tools should also be connected to national online safety apps, such as the 3018 application provided by e-Enfance, where such apps exist, as well as to the European Online Safety App when available. To ensure that minors are aware of the risks in the online environment, they should be informed of the specific risks prior to posting content or enhancing the visibility of certain content such as reposting content posted by other recipients. To that end, providers of online social networking services, of video-sharing platform services, AI companions, general conversational chatbots, and of online games, should, where appropriate, implement warning messages or other suitable measures aimed at informing minors before they undertake any actions.

(43) Guardians play an important role in the lives of minors, including in supporting their safe and informed navigation of the online environment. This is why guardians should be facilitated in providing such support through the availability of tools for guardians.

Tools for guardians are software, features, functionalities, or applications designed to help guardians accompany their minor's online activity, privacy, safety and well-being, while respecting children's agency and privacy. Tools for guardians should be considered as complementing other safety by design measures but should never replace the providers' own responsibility to ensure a high level of privacy, safety and security for minors. Since parental oversight is not always possible due to the realities of children's living arrangements and since guardians might be absent or disengaged, compliance should not depend exclusively on guardians. Tools for guardians should at least include features for reporting content on behalf of their child, setting screen time limits, seeing and being informed on the accounts that the minor communicates with, managing account settings, as well as other features to supervise uses of the services in scope of this Regulation that may be detrimental to the minor's privacy, safety and security. Such features may include warnings for guardians to be informed about potential repeated searches of minors related to suicide, self-harm, or eating disorders or initiate contact with or became friends with, including where such accounts belong to adults an adult. Where guardians manage minor's settings, they should be able to choose the time period for which they intend to change such settings. These tools should be tailored to the age of the minor, taking due account of their gradual development. Tools for guardians should be age-appropriate, easy to access and activate, effective and not easily circumvented, while respecting minors' rights to privacy, access to information and growing autonomy in accordance with their evolving capacities. For example, such tools should allow the guardian to use the tool without creating an account with the service and they should ensure that changes can only be made with the same degree of authorisation required for the initial activation of the tools. Minors should be clearly notified when such tools are activated and should, in particular where monitoring functionalities are used, receive a clear real-time indication. For very large online platforms within the meaning of Article 33(1) of Regulation (EU) 2022/2065, interoperability with third-party guardian tools should further enhance usability and effectiveness, in accordance with conditions set out by Article 6 of Regulation (EU) 2022/1925. The power to adopt acts in accordance with Article 290 TFUE should be delegated to the Commission in order to supplement this Regulation by laying down the necessary rules and technical criteria for the tools for guardians.

(44) Certain bodies, organisations and associations have particular expertise and competence in detecting and flagging suspected infringement of this Regulation and their complaints may have a positive impact on the freedom of expression and of the freedom of information in general. Therefore, guardians and minors should have the right to mandate such a body, organisation or association in accordance with the conditions set out in Article 86 of Regulation (EU) 2022/2065 to exercise the rights conferred by this Regulation on the minors' behalf. In addition to the right to lodge a complaint in accordance with Article 53 of Regulation (EU) 2022/2065, minors and guardians who are recipients of the service and users of systems and any body, organisation or association should have the right to lodge a complaint against providers subject to this Regulation. Such complaints should be lodged with the competent authority determined in accordance with Article 27 of the Member State where the recipient of the service is located or established, in accordance with national principles of good administration. For AI companions and general conversational chatbots, Article 85 of Regulation (EU) 2024/1689 should apply. The possibilities to contest decisions of providers of online platforms should leave unaffected in all respects the possibility to seek judicial redress in accordance with the laws of the

Member State concerned, and therefore should not affect the exercise of the right to an effective judicial remedy under Article 47 of the Charter.

(45) Ensuring a high level of protection of minors relies not only on the measures put in place by providers, but also, for providers of very large online platforms, on their ability to demonstrate through appropriate monitoring, testing and evaluating the effectiveness of the measures implemented in accordance with Chapter III, which should be part of the risk assessments conducted pursuant Article 34 of Regulation (EU) 2022/2065. Providers should consider the most up-to-date information available and insight from scientific and academic sources for that evaluation. To monitor and assess the effectiveness of the measures over time, providers should preserve all supporting documents relating to their evaluation for at least three years.

(46) To support the proper application of this Regulation, the Commission should encourage and facilitate the development, implementation, regular review and adaptation of voluntary Union-level codes of conduct involving, where appropriate, providers of online social networking services, video-sharing platform services, online games, AI companions, general conversational chatbots a, as well as competent authorities, civil society organisations, and other relevant stakeholders. Those codes of conduct should set out clear objectives, include specific commitments and reporting arrangements proportionate to the size and capacity of providers, and duly reflect the specific characteristics of the services concerned and the needs and interests of all parties, in particular minors. After consulting the European Board for Digital Services and the European Artificial Intelligence Board, within the scope of their respective competences, the Commission should assess, monitor and evaluate whether such codes are adequate to contribute to compliance with this Regulation.

(47) In the interest of clarity, simplicity and effectiveness, and to ensure the effective application and enforcement of this Regulation, providers of online social networking services, video-sharing platform services, online games, AI companions and, general conversational chatbots, which do not have an establishment in the Union should designate a legal representative in a Member State where they offer their services or systems. For simplification purposes, where such providers have already appointed a legal representative under Regulation (EU) 2022/2065 or Regulation (EU) 2024/1689, they should be able to fulfil that obligation by extending the mandate of that representative to cover all matters relating to the receipt of, compliance with and enforcement of decisions issued under this Regulation.

(48) Given the evolving nature of cross-cutting risks that minors may be exposed to within the online world, which is driven by constant innovation, the power to adopt acts in accordance with Article 290 TFUE should be delegated to the Commissions in order to amend the prohibitions on practices intended, or which can reasonably be foreseen, to encourage compulsive or excessive use of the service by minors, the measures ensuring that recommender systems are designed in way that ensures a high level of privacy, safety and security of minors, the default settings ensuring minors' accounts are set to a high level of privacy, safety and security, the measures ensuring a high level of privacy, safety and security of minors as regards contacts between minors and other recipients of the service, the measures limiting the visibility of any information shared by minors and their interactions with other recipients of the service, the measures ensuring a high level of protection of health, safety, fundamental rights and well-being of minors that may access AI companions and general conversational chatbot systems, the measures ensuring a high level of privacy, safety and security of minors on online games, and the measures ensuring agency for minors. This aims at

ensuring that the measures on safety by design remain effective and keep pace with practices Such amendments should be limited to what is necessary to address minors' privacy, safety and security.

(49) In order to verify the parental responsibility for the purpose of the creation of an account by the guardian for the benefit of a minor, providers should be able to use signals deriving from the publicly accessible databases at the Member States' level, such as those related to education or public birth registries, that the respective adult is a guardian of the minor concerned. Furthermore, in certain cases providers may already possess a signal that an adult is a guardian of a minor, such as in the case of past engagements with the service by the concerned minor and respective adult. In addition, adults should be able to self-declare that they exercise parental responsibility. Where such self-declaration is made, providers should make reasonable efforts to verify that the adult is the guardian of the minor concerned. Such verification should be carried out in a manner that respects data protection principles, particularly data minimization through the use of so-called 'zero knowledge proof', and should not lead to additional processing of personal data enabling the determination of the identity or tracking of the adult or minor concerned. This is without prejudice to the measures that the provider should be able to take to comply with its obligation under Article 18 of Regulation (EU) 2022/2065. The power to adopt acts in accordance with Article 290 TFUE should be delegated to the Commission in order to amend this Regulation by specifying the proof and signals that might indicate the parental responsibility. The Commission should be able to further explore technical and operational requirements for the possibility to include EU age verification as a tool for verification of parental responsibility.

(50) The assessment of the user's age is necessary for the effective implementation of the obligations laid down in this Regulation concerning registration with online social networking services, video-sharing platforms that are subject to a minimum age, access to age-inappropriate software applications and ensuring a high level of privacy, safety and security for minors through safety by design measures. The methods used should be accurate (such accuracy should be regularly assessed against appropriate, clear and publicly available metrics, under real-life circumstances and allow for correct determination of a user meeting the age threshold), reliable (for a method to be reliable, it should come from a reliable source, be available continuously at any time, and work in different real-world circumstances), robust (it should not be easy to circumvent), and should not be intrusive (not requiring recipients of the service to disclose their identity, precise age or other personal data where establishing that a relevant age threshold has been reached is sufficient) nor discriminatory (the chosen method should be appropriate and available for all users regardless of disability, language, ethnic, gender, religious and minority backgrounds). Where age assurance solutions do not meet these requirements, they should not be deemed compliant with this Regulation. Mere self-declaration by recipients of the service is not a sufficient age assurance solution for the purpose of compliance with this Regulation, and should not, on its own, be considered an appropriate nor effective measure when the protection of minors requires a reliable determination of age.

(51) The requirements of this Regulation on age assurance should be without prejudice to the application of Regulation (EU) 2016/679, notably the principles of purpose limitation and data minimisation as provided for in Article 5(1) points (b) and (c), thereof, as well as the requirements of data protection by design and by default. In particular, the requirements in this Regulation should not lead providers of services in

scope to maintain, acquire or process more personal data than strictly technically necessary to assess if the recipient of the service is a minor. In addition, providers of services in scope should not further process this information or combine it with additional data for any other purpose. Data protection obligations should be applicable both to providers of services in scope and any third party involved in age assurance, such as providers of age assurance solutions. To ensure the highest level of privacy and data protection, age assurance solutions used should be based on state-of-the-art technology and be zero knowledge proof.

(52) To avoid unnecessary friction for users and to limit the instances requiring age assessment, providers of software application stores and the providers of the services and systems subject to the obligations laid down in Chapter III should be able to store in relation to an account an age signal confirming that a user has already met a given age threshold. For providers of software application this means that no assurance has to be conducted for users that have already proven to have met the age threshold when trying to access or purchase software applications subject to the same or a lower threshold. The personal data processed in such age signals should be limited to what is strictly necessary for that purpose and should not be used for any other purpose.

(53) Age assurance is an umbrella term for different age assurance methods, including both age verification and age estimation. In order to ensure that recipients of the service have reached the minimum age, or where the service concerns a child-friendly service, providers of online social networking services or video-sharing platform services in scope of the access delay should put in place appropriate age verification solutions at the moment of account creation. To facilitate compliance and promote a trusted, interoperable and privacy-preserving approach to age verification across the Union, providers should exclusively use EU age verification solutions that rely on EU proof of age attestation that certified as conforming with the requirements of the EU Age Verification Scheme EU Age Verification Scheme, which is established in Commission Recommendation (EU) 2026/1035 and that are listed in the EU list of EU Verification Solutions and the EU list of providers of EU proof of age attestations. The EU Age Verification Solution relied upon by the providers should be provided by an independent third party. The standards and criteria necessary for highly effective age verification are set out on the EU Age Verification Scheme, and any third-party certified as conforming to this scheme should be considered as providing valid proofs of age. To ensure the highest level of privacy, security, accuracy, reliability and non-intrusiveness, providers of proof of age attestations and age verification solutions no other age verification solutions shall be deemed compliant with the obligations in the Regulation to assess the age than the EU Age Verification Solutions and EU proof of age attestations. These EU Age Verification Solutions and EU Proof of age attestations should meet the requirements of the EU age verification scheme, such as the use of Zero Knowledge Proof to prevent identity tracking and online linkability. Once it is established that the providers of the proof of age attestations and age verification solution meet those requirements, and notified as such by the Member States, they should be listed in the EU list of proof of age attestations and the EU list of EU age verification solutions.

(54) For the purpose of compliance with the safety-by-design requirements laid down in Chapter III, providers should also be allowed to use alternative age assurance solutions instead of age verification, where those solutions provide a high level of accuracy, reliability, security, robustness, non-intrusiveness, privacy, and non-discrimination.

(55) In cases when recipients of services and of systems referred to in paragraphs 1 and 4 consider that the outcome of the age assurance is incorrect, they should have access to an effective internal complaint-handling mechanism. That mechanism should enable complaints to be lodged by electronic means and free of charge, and should be easily accessible and user-friendly. In order to ensure effective redress, providers should handle such complaints diligently, impartially and without undue delay. Where a provider of an operating system has obtained, in compliance with this Regulation, an age signal of a user, that provider should, with the user's consent, enable the sharing of that age signal with providers in scope where this is necessary for compliance with this Regulation This should not lead to the processing of any additional data other than strictly necessary for the compliance with this Regulation. This obligation on providers of operating systems, should be without prejudice to the obligations for the providers to assess and verify the age to ascertain that the age signal has been obtained in accordance with the requirements set in this Regulation.

(56) For the purpose of ensuring uniform conditions for the application of the EU age verification scheme across the Union, implementing powers should be conferred on the Commission to lay down the specifications necessary as a basis for the functioning of the EU Age Verification Scheme, including the procedures for demonstrating and assessing conformity of the EU Age Verification solutions and the EU proof of age attestations by public authorities.

(57) In order to ensure uniform conditions for the application of alternative age assurance solutions, the power to adopt acts in accordance with Article 290 TFUE should be delegated to the Commission in order to supplement this Regulation by specifying the requirements and specifications necessary to ensure that an age assurance solution achieves a high level of accuracy, reliability, security, robustness, non-intrusiveness, privacy, and non-discrimination and specifying the requirements necessary to ensure the secure, privacy-preserving and interoperable sharing of age signals.

(58) Effective exercise of the possibility of the creation of a parental account for the benefit of a minor and for the effective use of tools for guardians under this Regulation requires adults with the parental responsibility to have access to the necessary means to prove such parental responsibility. Member States should therefore be required to 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. Such privacy-preserving electronic means should be effectively accessible to all guardians and minors residing in their territory, including persons with disabilities, persons with limited digital access or skills, and persons in vulnerable situations such as refugee and displaced families.

(59) No minor should be deprived of the protection under this Regulation, and no guardian of the means to exercise it, on account of the family's administrative, social or residence situation. Member States should therefore ensure that attestations of parental responsibility can also be obtained by families whose circumstances are not reflected in ordinary civil status records, including refugee and displaced families and legally appointed guardians of unaccompanied minors, on the basis of decisions or attestations issued by the competent authorities.

(60) Effective age verification across the Union requires recipients of the service to have access to suitable means of obtaining proof of age attestations. Without the availability of proof of age attestations, recipients of the service are prevented from accessing services solely because they lack access to a means to verify their age. Member States should therefore ensure the availability in their territory of different means of obtaining proof of age attestations, such as through biometric identity cards and passports, digital identity schemes, third party applications or in-person age verification. Member States should ensure that these means of obtaining proof of age attestation will enable the recipients to proof that they meet the age thresholds set in this Regulation a. This should include proof of age attestations for younger children Furthermore, Member States should ensure that an EU age verification solution is available free of charge. Member States should designate public authorities for the purposes of certifying EU age verification solutions and EU proof of age attestations. To that end, Member States should communicate to the Commission the names and addresses of the public authorities designated in their territory, together with any subsequent changes, and the Commission should make that information publicly available. Member States should also notify the Commission without undue delay of EU age verification solutions and EU proof of age attestations certified as conforming with the requirements of the EU Age Verification Scheme, together with the corresponding certificate of conformity, as well as of any subsequent suspension or withdrawal of such a certificate. In order to guarantee the effective and uniform application of this Regulation across the Union, an EU age verification solution or EU proof of age attestation that has been certified that has been included in the lists referred to in Article 30(1) should be recognised by all Member States. Member States should therefore not restrict or hinder, the use within their territory of an EU age verification solution that has already been included in that list by nomination of another Member State.

(61) The age requirements established by this Regulation should apply effectively to both new and existing accounts. Providers of services and systems subject to the minimum age should therefore establish, within an appropriate time period, whether recipients of services or users of systems holding existing accounts have reached the applicable minimum age. Providers should not be required to carry out a new age verification where they can establish with a high degree of confidence that the applicable minimum age has already been reached, including, where appropriate, on the basis of the date on which the existing account was created. The same principle should apply where providers are required to assess the age to distinguish adults from minors for the purposes of determining the parental responsibility and for providers of software applications stores to prevent minors from accessing or purchasing age inappropriate or by applicable Union law or national law adopted in compliance with Union age restricted applications. This approach is intended to avoid requiring all recipients of the service to undergo age verification or age assurance where there is already a high degree of confidence that a user is an adult, for example on the basis of reliable information such as through previously legitimately acquired credit card details. High confidence should be based on expected performance in practice on the full user base. In order to facilitate effective oversight of the implementation of these requirements by providers of very large online platforms, those providers should set out in advance how they intend to comply with these requirements concerning existing accounts and where applicable, how they intend to rely on the relevant exceptions.

(62) In order to ensure that existing accounts are brought into compliance with the minimum age obligations, providers of very large online platforms should before the

expiry of the six month time period, submit to the competent authority a detailed implementation plan that corroborates the required high degree of confidence. To this end, the plan should set out a schematic description of the complete process pipeline used to determine the age of existing users, together with a clear account of each technical tool or measure and the underlying decision rules. Where relevant, it should be supported by robust evidence of performance under real-life circumstances derived from a statistically representative sample of the full user base – the representativeness of the sample with respect to the relevant age signals should be demonstrated – and should present accuracy, precision and recall for underage recipients as well as a full confusion matrix with granular age buckets, together with a description of how the sample and the age labels were obtained. Where the year of account creation is relied upon as a derogation, the plan should additionally provide empirical evidence and the statistical confidence that this single signal is sufficient to infer that the user has reached the applicable minimum age. The plan should also outline how the provider will monitor that the expected performance has been achieved, for example through a post-implementation audit. Finally, the plan should demonstrate that the proposed measures respect the general age-assurance principles of this Regulation, including accuracy, reliability, security, robustness, non-intrusiveness, privacy and non-discrimination.

(63) Recognising that effective protection of minors requires not only regulatory measures but also awareness, education and empowerment, Member States should establish national strategies building on the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the Regions: A digital Decade for children and your: the new European strategy for a better internet for kids (BIK+) of 11 May 2022 and its network of Safer Internet Centres with awareness activities, helplines supporting children, guardians and educators and hotlines to report suspected illegal content. Notably, Member States should promote the development of minors' digital literacy skills so that, by the time they reach the minimum age, they are able to understand the risks of the online environment covered by this Regulation, to use digital services and systems safely and critically, and to make informed use of the protections, settings and tools that providers are required to make available. Minors, and their guardians, should have easy, free and confidential access at national level to channels through which minors can seek assistance in relation to the harms addressed by this Regulation, including unwanted contact and cyberbullying in line with the 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" of 10 February 2026. Those channels should complement the reporting and support tools provided pursuant to this Regulation, be capable of providing rapid assistance, and direct minors to further sources of support available at national level. It should be possible to support these activities, including those carried out by the Safer Internet Centres, by Union funding made available under the relevant Union programmes and instruments established under the multiannual financial framework, such as the National and Regional Partnership Plans. In order to support effective implementation, Member States should communicate the measures taken to the Commission, and the Commission should facilitate the exchange of best practices between Member States.

(64) This Regulation should specify certain provisions of Regulation (EU) 2022/2065. In order to ensure effective supervision and enforcement of this Regulation, Chapter IV of Regulation (EU) 2022/2065 should apply to the extent that the relevant provisions

regulate providers of intermediary services in scope of that Regulation. The Commission should have exclusive powers to supervise and enforce obligations laid down in this Regulation that apply to providers of very large online platforms within the meaning of Article 33 of Regulation (EU) 2022/2065.

(65) Similarly, to avoid overlaps and ensure consistency with the existing horizontal framework applicable to AI systems under Regulation (EU) 2024/1689, the enforcement of the specific safety requirements provided for in this Regulation for AI companions and general conversational chatbots should be based on the supervisory and enforcement framework and procedures set out in Regulation (EU) 2024/1689.

(66) Providers of online games that are video gaming platforms are subject to the supervision and enforcement structure pursuant to Regulation (EU) 2022/2065. In order to ensure coherence with enforcement under this Regulation, the competent authority responsible for the supervision of providers of online games that are video games should be a competent of the Member State of main establishment of the provider.

(67) In order to ensure legal certainty and consistent application throughout the Union, and to avoid fragmentation of the internal market resulting from divergent national interpretations, Member State authorities should not adopt decisions that run counter to a decision taken by the Commission pursuant to this Regulation. The Commission, Digital Services Coordinators and competent authorities, where applicable, should work in close cooperation and coordinate their enforcement actions to ensure coherent, effective and complementary enforcement of this Regulation on the one hand, and Regulations (EU) 2022/2065 and 2024/1689 on the other, including by drawing on the cooperation and consistency mechanisms established in Chapter IV of Regulation (EU) 2022/2065.

(68) The Commission should aim to adopt a final decision within 90 days from the opening proceedings for suspected infringements of this Regulation. It should also communicate its preliminary findings to the provider concerned within 30 days from opening proceedings.

(69) The Commission should be in possession of all the necessary resources, in terms of staffing, expertise, and financial means, for the performance of its tasks under this Regulation. In order to ensure the availability of the resources necessary for the adequate supervision at Union level under this Regulation the Commission should charge an annual supervisory fee, the level of which should be established on an annual basis, on providers of online social networking services, video-sharing platform services, of software application stores and of AI companions and of general conversational chatbots, which it enjoys the competence to supervise with regard to compliance with Chapters II to V of this Regulation and that are designated as very large online platforms pursuant to Article 33 of Regulation (EU) 2022/2065. The annual supervisory fee required for the enforcement of this Regulation vis-à-vis those providers should be integrated in the supervisory fee charged to such providers of very large online platforms pursuant to Article 43 of Regulation (EU) 2022/2065. Similarly to that supervisory fee, the external assigned revenues resulting from the annual supervisory fee under this Regulation should cover additional human resources in the Commission, including officials, contract agents and national experts. Finally, the cap on the supervisory fee introduced in this Regulation should be taken together with the cap laid down in Regulation (EU) 2022/2065 and should ensure that overall resources

of the Commission are sufficient to carry out its tasks under this Regulation and Regulation (EU) 2022/2065.

(70) The overall amount of the annual supervisory fee under this Regulation should include costs related to the exercise of the Commission's specific powers and tasks of supervision, monitoring, investigation, and enforcement in respect of the providers of the very large online platforms and search engines covered by this Regulation. In particular, it should include the costs related to the set-up, maintenance and operation of the EU Age Verification Scheme, including funding related to activities concerning the roll out the EU Age verification solution across the EU and the development of expertise and capabilities pursuant to Article 36. However, the individual annual supervisory fee should not exceed an overall ceiling for each provider of very large online platforms taking into account the economic capacity of the provider of the designated service or services.

(71) The Commission should apply the rules and principles laid down in Article 43 of Regulation (EU) 2022/2065 when charging the annual supervisory fee under this Regulation.

(72) In view of the importance of protecting children, the Commission, in cooperation with the Digital Services Coordinators and the Board, should develop the Union expertise and capabilities as regards the supervision of services in scope of this Regulation.

(73) Given the importance of the impact of the services and systems in scope of this Regulation on the protection of minors, the failure of the providers to ensure a high level of privacy, safety and security and comply with the specific obligations applicable to them may rapidly come to seriously affect a substantial number of minors using their services or systems across different Member States and may cause substantial harms, while such failures may also be particularly complex to identify and address timely. The Commission, in cooperation with the competent authorities, should develop the Union expertise and capabilities, including establishing knowledge sharing networks, to respond quickly to such incidents affecting the protection of minors. Such incidents should be understood as fast-evolving situations taking place within or outside the EU, with an online dimension and presumed connection to the scope of this Regulation, that seriously and negatively affect the privacy, safety, security or health and well-being of minors the service in the Union, and that requires an immediate response, such as dangerous or harmful challenges circulating among minors and posing them at immediate risk. The Commission should therefore be able to coordinate and rely on the expertise and resources of competent authorities, for example by analysing, on a permanent or temporary basis, specific trends or issues emerging regarding those fast-evolving situations which impact minors' health, well-being, privacy, safety, and security. Member States should cooperate with the Commission in developing such capabilities, including through secondment of personnel where appropriate, and contributing to the creation of a common Union supervisory capacity, as well as an administrative arrangement setting out procedures to facilitate a rapid response in the event of an incident affecting the protection of minors. Member States should establish minimum preparedness levels for national authorities to ensure regular communications channels between relevant national authorities and third parties and map and where relevant incident reaction protocols at national level.

(74) This Regulation respects the fundamental rights, including children's rights, recognised by the Charter and the fundamental rights constituting general principles of

Union law. Accordingly, this Regulation should be interpreted and applied in accordance with those fundamental rights, including the respect for private and family life enshrined in Article 7 of the Charter, to the protection of personal data enshrined in Article 8 of the Charter, to freedom of expression and information, including the freedom and pluralism of the media, enshrined in Article 11 of the Charter, to non-discrimination enshrined in Article 21 of the Charter, to respect for the rights of the child enshrined in Article 24 of the Charter. When exercising the powers set out in this Regulation, all public authorities involved should achieve, in situations where the relevant fundamental rights conflict, a fair balance between the rights concerned, in accordance with the principle of proportionality.

(75) Since the objectives of this Regulation, namely to contribute to the proper functioning of the internal market and to ensure a high level of privacy, safety, and security of children cannot be sufficiently achieved by the Member States because they cannot achieve the necessary harmonisation and cooperation by acting alone, but can rather, by reason of territorial and personal scope, be better achieved at the Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve those objectives.

(76) The European Data Protection Supervisor was consulted in accordance with Article 42(2) of Regulation (EU) 2018/1725 of the European Parliament and of the Council, and delivered its opinion on [DATE].

HAVE ADOPTED THIS REGULATION:

CHAPTER I – GENERAL PROVISIONS

Article 1 – Subject matter

This Regulation contributes to the proper functioning of the internal market and ensures a high level of protection for minors online in the Union by setting out harmonised rules for a safe and empowering online environment for minors, including the principle of consumer protection. It specifies and complements Regulation (EU) 2022/2065, and complements Regulation (EU) 2024/1689. In particular, this Regulation establishes:

(a) a harmonised minimum age for creating an account with online social networking services and video-sharing platform services;

(b) harmonised safety requirements for online social networking services, video-sharing platform services, video gaming platforms, and software application stores and harmonised safety requirements to protect minors online for video games, AI companions and general conversational chatbots;

(c) harmonised rules regarding age assurance online.

Article 2 - Scope

1. This Regulation applies to providers of the following services or systems accessible to minors:

   (a) online social networking services;

   (b) video-sharing platform services;

(c) software application stores

(d) online games;

(e) operating systems;

(f) AI companions;

(g) general conversational chatbots.

2. For the services referred to in paragraph 1 points (a) to (e), this Regulation applies to providers of services irrespective of where they have their place of establishment where they offer those services to recipients of the service that have their place of establishment or are located in the Union.

3. For the AI systems referred to in paragraph 1 points (f) and (g), this Regulation applies to providers placing on the market or putting into service such AI systems in the Union, irrespective of where those providers are established or located.

4. This Regulation does not apply to the providers of any of the following:

(a) not-for-profit online encyclopaedias;

(b) not-for-profit educational and scientific repositories;

(c) services and systems that are designed for primarily educational purposes, and operated by educational establishments or organisations, or on their behalf;

(d) open-source software-developing and-sharing platforms, unless the platform itself constitutes an AI system in scope of this Regulation or Regulation (EU) 2024/1689;

(e) services and systems specifically developed and operated for the sole purpose of scientific research and development;

(f) services and systems designed, developed and operated by public authorities and for exclusive use of those public authorities or on their behalf.

5. Where justified in view of the potential risks to the privacy, safety and security of minors posed by a service or a system or where a service or a system poses such a risk that is equivalent to, or lesser than, the risks posed by the services or systems already referred to in paragraph 4, the Commission is empowered to adopt delegated acts in accordance with Article 40 to amend paragraph 4 of this Article by adding other types of services or systems to the list of exempted services or systems or removing services or systems from that list.

6. Providers of online social networking services, video-sharing platform services, and video gaming platforms subject to Article 28(1) of Regulation (EU) 2022/2065 that comply with the obligations laid down in this Regulation shall be deemed to comply with that Article for matters covered by this Regulation, including as regards AI systems that are deployed as a functionality of online platforms in scope of Article 28(1) of Regulation (EU) 2022/2065 in the provision of that service.

7. This Regulation is without prejudice to the rules laid down by other Union legal acts regulating other aspects of the provision of intermediary services and Union legislation applicable to AI systems in the internal market, including the following:

(a) Directive 2010/13/EU[8];

(b) Union law on consumer protection and product safety, including, Directives 2005/29/EC, 2011/83/EU, (EU) 2019/770, Council Directive 93/13/EEC, and Regulations (EU) 2019/1020, (EU) 2023/988 and (EU) 2024/1689;

(c) Union law on the protection of personal data, in particular Regulation (EU) 2016/679 and Directive 2002/58/EC;

(d) Directive (EU) 2024/1385.[9]

Article 3 - Definitions

1. For the purposes of this Regulation, the definitions of 'online platform', 'recipient of the service', 'online interface', 'recommender system' set out in Article 3 of Regulation (EU) 2022/2065 shall apply.

2. For the purposes of this Regulation, the definitions of 'online social networking service', 'video-sharing platform service', and 'software application store' set out in Article 2 of Regulation (EU) 2022/1925 shall apply. Those services shall be considered an 'online platform' within the meaning of Article 3, point (i), of Regulation (EU) 2022/2065 for the purpose of this Regulation.

3. For the purposes of this Regulation, the definitions of 'AI system' and 'general-purpose AI system' offset out in Regulation (EU) 2024/1689 shall apply; the definition of 'provider' as defined in Article 3 point (3) of that Regulation shall apply with regard to AI systems regulated by this Regulation.

4. For the purposes of this Regulation, the definition of 'operating system' set out in Article 2, point (1), of Regulation (EU) 2022/1925 shall apply.

5. For the purposes of this Regulation, the following additional definitions shall apply:

(a) 'minor' or 'child' means any natural person under the age of 18;

(b) 'guardian' means any person holding parental responsibility over a minor pursuant to applicable national law;

(c) 'AI companion' means an AI system, including a general-purpose AI system, that provides sustained, personalised interaction or companionship which simulates or facilitates a social, emotional or interpersonal relationship with a user;

(d) 'general conversational chatbot' means a general-purpose AI system with general conversational functionalities for direct interaction with users that is capable of providing assistance across multiple domains and tasks; this definition excludes AI systems whose conversational functionality is limited to a specialised service, task or pre-defined set of functions, including specialised customer-service, business operation, technical-support, transactional, educational, information-retrieval, industrial or manufacturing AI applications;

---

8 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, p. 1, ELI: http://data.europa.eu/eli/dir/2010/13/oj).

9 Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence (OJ L, 24.05.2024, p. 1, ELI: http://data.europa.eu/eli/dir/2024/1385/oj).

(e) ‘online games’ means a video game or video gaming platform;

(f) ‘video game’ means an information society service as defined in Article 1(1), point (b), of Directive (EU) 2015/1535, that allows the recipients of the service to engage, by means of application accessed locally or remotely, including through the use of a durable medium and that involves interaction with a user interface or input device to generate visual feedback from a display device in a simulated environment for play or entertainment purposes;

(g) ‘video gaming platform’ means an “online platform" as defined in Article 3, point (i) of Regulation (EU) 2022/2065, that involves interaction with a user interface or input device to generate visual feedback from a display device in a simulated environment [for play or entertainment purposes];

(h) ‘age verification’ means a process or system for establishing, with a high degree of certainty, whether the recipient or user of a system of the service has attained a specific age or age threshold, on the basis of information derived from identification documents or other reliable, verified sources of identification;

(i) ‘age assurance’ means the set of methods, that can be used to determine, estimate or verify the age of a natural person, encompassing age estimation and age verification and excluding self-declaration by recipients of the service;

(j) ‘age signal’ means any data, attribute, token, credential, or other information provided, transmitted, or generated for the purpose of establishing, verifying, or demonstrating a specific age, age threshold, or age range of an individual;

(k) ‘EU age verification solution’ means an age verification solution that meets the requirements of the EU Age Verification Scheme and is certified by a public authority and included in the EU list of EU age verification solutions after notification by a Member State;

(l) ‘EU list of providers of EU proof of age attestations’ means the list established and published by the Commission of providers issuing EU proof of age attestations

(m) ‘EU list of EU age verification solutions’ means the list established and published by the Commission of EU age verification solutions certified as conforming with the EU Age Verification Scheme and notified by Member States;

(n) ‘EU Age Verification Scheme’ means a scheme for the attestation of attributes as defined in Article 2(4) of Commission implementing Regulation (EU) 2025/1569 with the rules applicable to providers of EU age verification solutions and of EU proof of age attestation, their approval and inclusion in the EU list of providers of EU proof of age attestations and the certification of EU age verification solutions for their inclusion in the EU list of EU age verification solutions;

(o) ‘proof of age attestation’ means an electronic attestation of attributes, as defined in Article 3(44) of Regulation (EU) No 910/2014, that allows the authentication of the fact that its holder meets a given age, age threshold, or age range;

(p) ‘tools for guardians’ means software, features, functionalities, or applications designed to help guardians accompany minors' online activity to ensure their privacy, safety and well-being.

Article 4 – Anti-circumvention

Providers of online social networking services, of video-sharing platform services, of online games, of software application stores, of operating systems, of AI companions, and of general conversational chatbots:

(a) shall not engage in any behaviour that undermines effective compliance with their respective obligations under this Regulation, regardless of whether that behaviour is of a contractual, commercial or technical nature, or of any other nature, or consists in the use of behavioural techniques or interface design;

(b) shall be prohibited from taking knowingly and intentionally any other actions whose object or effect is, directly or indirectly, to circumvent their respective obligations under this Regulation, with a view to avoiding compliance with those obligations.

Article 5 – Notification and independent audit of a compliance plan

1. Within 4 months following the notification of the decision designating them as a very large online platform pursuant to Article 33 of Regulation (EU) 2022/2065, the providers of online social networking services and video-sharing platform services that have been designated as a very large online platform pursuant to Article 33 of Regulation (EU) 2022/2065 shall notify to the Commission a compliance plan describing in a detailed manner compliance with the obligations laid down in Chapters II to V of this Regulation.

   For providers referred to in the first sub-paragraph already designated as a very large online platform pursuant to Article 33 of Regulation (EU) 2022/2065, such notification shall occur within 30 days from the date of the entry into application of this Regulation.

   Article 34(3) of Regulation (EU) 2022/2065 shall apply mutatis mutandis to the supporting documents of those notifications.

2. For the purpose of enabling the Commission to assess the compliance of providers referred to in paragraph 1 with the obligations laid down in Chapters II to V, those providers shall, at their own expense, commission an audit of the compliance plan notified pursuant to paragraph 1 by one or more independent auditors. The independent auditors shall have, or shall retain experts with proven expertise in the following areas relevant for the protection of minors:

   (a) protection and rights of the child;

   (b) paediatric medicine and child psychiatry;

   (c) developmental science;

   (d) age assurance;

   (e) the design of online interfaces and recommender systems;

   (f) data protection and security.

3. Article 37(2) and (3) of Regulation (EU) 2022/2065 shall apply mutatis mutandis to the audits carried out pursuant to this Article and to the independent auditors and any experts retained by them. The costs of the audit shall be borne by the provider concerned. These costs shall not exceed market rates for comparable assessments by the auditors.

The providers referred to in paragraph 1 shall cooperate with the independent auditors and shall grant them access to all information, data, documents and personnel relevant for the performance of the audit.

Providers shall ensure that any employee or contractor that has communicated with the independent auditor are protected against any adverse action by the provider.

4. The independent auditors commissioned by the provider pursuant to paragraph 2 shall:

(a) assess the compliance plans submitted by the providers pursuant to paragraph 1 in view of the obligations laid down in Chapters II to V;

(b) transmit a draft report to the provider, which may submit comments within 15 days of receipt;

(c) issue a final report, taking into account any comments received pursuant to point (b), simultaneously to the Commission and to the provider, within two months of receipt of the compliance plan, identifying any shortcomings in the compliance measures described therein.

5. The provider concerned shall publish, without undue delay after its receipt, a summary of the final report referred to in paragraph 4, point (c), which shall not contain confidential information.

6. Where the Commission concludes by means of a decision on the basis of the final report referred to in paragraph 4, point (c) that the compliance plan contains shortcomings, the provider concerned shall submit to the Commission and to the independent auditor within 30 days of the receipt of the Commission decision report a corrective action plan identifying one or more corrective measures for each identified shortcoming.

The provider shall also identify a reasonable period, which shall not be longer than 60 days, for the implementation of each corrective measure in the corrective action plan.

The independent auditor shall verify the implementation of the corrective measures and shall report thereon to the Commission and to the provider concerned.

7. In assessing the compliance of the providers referred to in paragraph 1 with the obligations laid down in Chapters II to V of this Regulation, the Commission shall be entitled to consider the compliance plan referred to in paragraph 1, the final report referred to in paragraph 4, point (c) and any corrective measures communicated pursuant to paragraph 6 or any other information that the Commission may consider relevant.

8. Neither the final report referred to in paragraph 4, point (c), nor any action or absence thereof by the Commission in relation to that final report or to the compliance plan shall constitute a finding of compliance with the obligations laid down in Chapters II to V of this Regulation, or shall limit the powers of the Commission under this Regulation or under Regulation (EU) 2022/2065.

9. Providers shall, after the first notification pursuant to paragraph 1, report annually on their compliance with the obligations laid down in Chapters II to V of this Regulation as part of their annual risk assessments carried out pursuant to Article 34 of Regulation (EU) 2022/2065.

   Compliance with the obligations laid down in Chapters II to V of this Regulation shall be included in the independent audits carried out pursuant to Article 37 of Regulation (EU) 2022/2065.

10. This Article is without prejudice to the powers of the Commission under this Regulation and under Regulation (EU) 2022/2065, including the power to adopt interim measures.

11. The Commission may adopt implementing acts laying down templates and methodologies for the audits carried out pursuant to this Article. Those implementing acts shall be adopted in accordance with the procedure referred to in Article 39.

CHAPTER II – DELAYED CREATION AND USE OF ACCOUNTS FOR MINORS ON ONLINE SOCIAL NETWORKING SERVICES AND VIDEO-SHARING PLATFORM SERVICES

SECTION I – Delayed access for minors

Article 6 – Delayed creation and use of accounts

1. Providers of online social networking services and of video-sharing platform services shall not allow a natural person below the age of 15 years to create an account with that service or to access that service by means of an account, created for, or attributed to, that person, where the service poses a risk to the privacy, safety or security of a minor below that age.

   A service shall be considered to pose a risk to the privacy, safety or security of minors below 15 years of age where it meets any of the following conditions:

   (d) enables recipients who access the service through an account to transmit content in real-time to an indeterminate number of other recipients of the service, including through live streaming of audio-visual content;

   (e) enables recipients who access the service through an account to contact, communicate and otherwise interact with other recipients of the service not part of the recipient's pre-existing connections or subscriptions;

   (f) uses a recommender system which is based on profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679;

   (g) uses a recommender system suggesting or prioritising to a recipient who accesses the service through an account contact suggestions or information that has not been provided by one of the recipient’s pre-existing connections or subscriptions;

   (h) deploys or presents functionalities, interface designs or characteristics which are intended, or can reasonably be foreseen, to enable uninterrupted content consumption, that incentivise interactions with the service or with content or other recipients of the service, or that transmit automated notifications designed to prompt the user to initiate or resume use of the service.

2. By way of derogation from paragraph 1, providers of online social networking services and video-sharing platform services may allow guardians to set up accounts for minors above the age of 13 years and below the age of 15 years with limited features so as to allow them to access the service by means of such a limited account. Such accounts shall meet at least the following conditions

   (a) the tools for guardians provided for in Article 20 shall always be activated;

   (b) guardians are enabled to set a maximum limit on the amount of time in a day the service or system may be accessed through that account, which shall not exceed one hour per day;

   (c) guardians are enabled to pre-approve potential new contacts and to set a maximum limit on the number of other recipients or users in the account's contacts.

3. When creating an account for a minor pursuant to paragraph 2 of this Article, the provider of online social networking services and of video-sharing platform services shall take measures to establish whether the person creating the account is the holder of parental responsibility over that minor in accordance with Article 26 and verify that the recipient of the service has reached the age of 13 years in accordance with Article 28(1).

4. Providers of services falling within scope of paragraph 1 of this Article shall by 6 months after the entry into application of this Regulation establish whether the holders of existing accounts used to access their service are below the age of 15 years. Where holders of existing accounts are established to be below 15 years, providers of services concerned shall disable the accounts of the recipients or users of the service that have been established to be below that age or in relation to whom the age cannot be established.

5. Where providers of services falling within scope of paragraph 1 process personal data pursuant to Article 6(1), point (a) of Regulation (EU) 2016/679, the provisions set out in this Article should apply in parallel to the age limits provided in Article 8 of that Regulation.

6. The Commission may adopt delegated acts, in accordance with Article 40, in order to amend this Regulation by modifying and complementing the conditions in paragraph 1 of this Article, to include new features and functionalities or changes to existing features or functionalities that pose a risk to minor's privacy, safety, and security online equivalent to the risks posed by the conditions set out in paragraph 1 of this Article.

SECTION II – Guardian-controlled access for minors below age of 13 years

Article 7 – Guardian-controlled access for minors below the age of 13

1. Providers of video-sharing platform services whose service is specifically designed for minors below the age of 13 years may exceptionally enable a guardian to allow a minor below the age of 13 years limited access to the service through the guardian's own account, where all of the following conditions are met:

   (a) such guardian-controlled access shall take place exclusively through the guardian's own account, and no account shall be created for, or attributed to, the minor;

(b) such access shall be enabled and controlled by means of the tools for guardians referred to in Article 20 or other parental control settings in the guardian's account or on the guardian's device;

(c) the provider expressly permits, in its terms and conditions, access by minors below the age of 13 years, clearly specifying therein the age range of minors for whom access is permitted subject to guardians' approval;

(d) the provider has carried out and published, in at least one official language of a Member State and in a publicly available section of its online interface, an assessment of the impact of the service, or of the relevant parts thereof, on minors within the specified age range, assessing the risks and demonstrating, if applicable, how any such risks have been effectively mitigated taking into account the relevant age groups. Compliance with the requirements set out in Chapter III shall not automatically entail effective mitigation of such risks;

(e) the provider has set out, in a clear and transparent manner in a publicly available section of its online interface, which content or behaviour is considered as not age-appropriate or harmful to the privacy, safety and security of minors within the specified age range on the service;

(f) access to the content identified pursuant to point (e) shall not be granted to minors below the age of 13 years;

(g) the available features and functionalities are adapted, and gradually adjusted, to the age of the minor declared pursuant to paragraph 4, point (b);

(h) all personalisation features and recommender systems, and any functionality to search for content shared by other recipients of the service, are turned off and cannot be activated, unless the assessment referred to in point (d) demonstrates that their activation is in the best interests of the minor and does not in any way negatively affect the minor's privacy, safety and security.

2. Nothing in this Article shall be construed as requiring a provider to permit access by minors below the age of 13 years, or as conferring on any minor or guardian a right of access to a service whose terms and conditions do not permit such access or where access to the service is subject to a higher minimum age under EU law or national law in compliance with EU law.

3. The account through which guardian-controlled access pursuant to paragraph 1 is provided shall be set up, registered and held exclusively by the guardian. The minor accessing the service through the guardian's account shall not be a party to the contract with the provider. The provider shall take measures to establish that the guardian enabling access pursuant to paragraph 1 is the holder of parental responsibility in respect of the minor concerned, in accordance with Article 26.

4. The design and functioning of the guardian-controlled access provided pursuant to this Article shall not disproportionately restrict the minor's privacy and shall support the minor's autonomy and agency, in accordance with the minor's evolving capacities. The guardian-controlled access provided pursuant to this Article shall meet at least the following conditions:

(a) the tools for guardians provided for in Article 20 shall be activated by default;

(b) the guardian shall declare the age of the minor for whom access is enabled and such access shall not be enabled for a minor below the age of 3 years;

(c) the guardian shall be able to set a maximum daily duration of access by the minor, which shall not exceed one hour;

(d) the guardian shall be able to supervise the content displayed or recommended to the minor, taking into account the minor's right to privacy and taking the minor's best interests as a primary consideration;

(e) the guardian shall be able to approve, limit and remove any other recipients of the service with whom the minor may interact through the guardian's account;

(f) the guardian shall be able to suspend the minor's access at any time.

5. Guardian-controlled access pursuant to this Article shall be discontinued when the minor reaches the age of 13 years, to be determined on the basis of the age declared pursuant to paragraph 4, point (b) of this Article. This shall be without prejudice to the creation of an account pursuant to Article 5(2) where the conditions of that Article are met.

6. The Commission may adopt delegated acts in accordance with Article 40 in order to amend this Regulation by adapting to technological and scientific developments the conditions set out in paragraphs 1 and 4, where such changes maintain a level of protection of the minor's privacy, safety, and security online equivalent to that provided by the conditions set out in paragraphs 1 and 4 of this Article.

CHAPTER III – SAFETY BY DESIGN

SECTION I – General obligation on safety by design

Article 8 – General obligation on safety by design

1. Providers of online social networking services, of video-sharing platform services, of online games, of AI companions, of general conversational chatbots, and of software application stores, regardless of whether those services or systems are accessible with an account, and including services and systems accessible through the accounts specified in Article 5(3) and Article 6(3), shall ensure a high level of privacy, safety and security of minors. Providers of such services or systems shall design those services and systems in accordance with the requirements laid down in this Chapter by default and shall only derogate from those requirements after they have established that the recipient of the service or the user of the system is an adult, by making use of age assurance in accordance with Chapter V.

2. Compliance with the obligations set out in this Chapter shall be without prejudice to the obligation of providers of online social networking services and of video-sharing platform services to delay the creation of accounts pursuant to Article 6 and shall be without prejudice to the obligation of providers of video-sharing platform services concerning guardian-controlled access for minors, where applicable, pursuant to Article 7.

3. Where providers of online social networking services or of video-sharing platform services deploy AI companions or general conversational chatbots as a functionality in the provision of those services, only the obligations set out in Sections III, V and VI shall apply to such AI systems.

SECTION II – Obligations for online social networking services and video-sharing platform services

Article 9 – Addictive design

1. Providers of online social networking services and of video-sharing platform services shall not design, organise or operate their services in a manner that is intended, or can reasonably be foreseen, to encourage compulsive or excessive use of the online social networking services and of video-sharing platform services by minors.

2. The following features shall be deemed to encourage compulsive or excessive use of the service by minors within the meaning of paragraph 1:

   (a) enabling automatic play of content and uninterrupted content consumption without effective and regular interruption moments that enable deliberation by the minor on their willingness to consume more content;

   (b) undermining the minor's decision to discontinue use of the service or not providing minors with the ability to take such decision, such as notifications not triggered by, or not directly related to, the minor's interaction or activity on the service;

   (c) incentivising or rewarding minors to share content or to engage in real-time transmission of content to an indeterminate number of recipients of the service;

   (d) incentivising engagement at regular times or with greater frequency, including through penalties or loss of benefits for failing to engage regularly or within specified time intervals.

3. Providers of online social networking services and of video-sharing platform services shall put in place effective measures to ensure:

   (a) time-limited access for minors on their service;

   (b) interruption of usage by minors on their service.

   Such measures shall be designed in a way that protects school time and core sleep hours of minors.

Article 10 – Recommender systems

1. Providers of online social networking services and of video-sharing platform services that use recommender systems shall design the information suggested and the optimisation of their recommender systems to minors in way that ensures a high level of privacy, safety and security of minors.

2. For the purpose of complying with the obligations set out in paragraph 1 of this Article, providers of online social networking services and of video-sharing platform services that use recommender systems shall ensure that the recommender system optimisation does not exploit minor's vulnerability or attention and that it includes evaluation metrics capturing quality, safety and mental health outcomes for minors, by taking at least the following measures:

   (a) ensure that the recommender systems give priority and primary weight to explicit user-stated preferences when suggesting information;

   (b) disable by default the recommendation of information suggested by the recommender system based on implicit engagement-based signals from minors' behaviour online;

   (c) ensure that the recommender systems do not rely on the collection of any personal data of minors captured from outside the service;

(d) ensure that minors are not exposed to information suggested by the recommender systems that may pose a risk to their privacy, safety and security, including if encountered repeatedly.

3. Providers of online social networking services and of video-sharing platform services that use recommender systems shall provide and prominently display tools that enable minors to:

(a) modify or control the parameters of the recommender system, including by easily deleting all previous identified preferences;

(b) choose at least one option of the recommender systems which is not based on profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679.

Tools referred to in the first subparagraph shall not be designed in a manner to entice minors into choosing the option based on profiling, shall be offered during account creation and shall remain directly accessible from the specific section of the service's online interface where the information is being prioritised, including for recipients of the service without an account.

Article 11 – Safe settings

1. Providers of online social networking services and of video-sharing platform services shall put in place measures to ensure that settings are set by default to a high level of privacy, security and safety of minors. To ensure compliance with this paragraph, such providers shall, by default, turn off at least the following settings:

(a) geolocation and other tracking features;

(b) access to microphone and camera;

(c) recommendations of other accounts and synchronisation of contacts;

(d) push notifications, which should, in any event, be designed in a way that protects minors' core sleep hours and school time.

2. Default settings referred to in paragraph 1 may only be changed by the provider where the minor is above the age of 15 years and was clearly and unambiguously informed about such changes and has explicitly consented to such changes. Default settings referred to in paragraph 1 point (a), where enabled by minors, shall be turned off after their session on the service ends.

3. Where features or settings pose a risk to minors' privacy, safety security or health and well-being providers of online social networking services and video-sharing platform services shall ensure that those features or settings are not available to minors. This shall at least include features increasing social comparison or misrepresenting minors' image, in particular by disproportionately embellishing or idealising it.

Article 12 – Contact and interaction safeguards

1. Providers of online social networking services and of video-sharing platform services shall put measures in place that ensure a high level of privacy, safety and security of minors as regards contacts between minors and other recipients of the service. Those measures shall at least ensure that:

(a) other recipients of the service are not able to initiate direct contact with the minor, if the minor has not pre-approved such contact.

(b) minors with an account are not included in contact recommendations or similar features aiming to enable other recipients of the service, including minors, to expand their contacts;

(c) minors can only be added to a group with a limited or unlimited number of recipients of the service after their explicit agreement;

(d) minors can easily block any other recipient of the service without having their identity disclosed to the blocked recipients of the service.

2. Providers of online social networking services and of video-sharing platform services shall implement safeguards to prevent recipients of their service from enticing or manipulating minors into approving the direct contact referred to in paragraph 1, point (a).

3. Providers of online social networking services and of video-sharing platform services shall put in place measures to limit the visibility of any information shared by minors and their interactions with other recipients of the service. Those measures shall include at least the following:

(a) by default, other recipients of the service not previously accepted by the minor shall not be able to access account information of the minor or content uploaded or shared by the minor on the service;

(b) recipients of the service without an account shall not be able to access account information of minors or content uploaded or shared by minors on the service;

(c) the personal contact details of minors, such as their name, phone number, e-mail address and address, shall not be disclosed to or shared with other recipients of the service;

(d) minors shall be able to easily control the visibility of any content shared, interaction and related metrics on the service;

(e) other recipients of the service shall not be able to download or take screenshots of contact, location or account information of minors or of any content uploaded or shared by minors on the service;

(f) minors shall, by default, not be able to host real-time transmission of user-generated content, including through live-streaming of audiovisual content.

Article 13 – Safety and security of economic transactions

1. Providers of online social networking services and of video-sharing platform services shall ensure that, before an economic transaction takes place, a minor is made aware in a clear and easily comprehensible manner, and in real time, that this is an economic transaction. Purchases carried out within the service with virtual currency purchasable with funds within the meaning of Article 4, point (25) of Directive (EU) 2015/2366 shall display the corresponding monetary value in the official currency of the Member State in which the recipient of the service is habitually resident.

2. Providers of online social networking services and of video-sharing platform services shall not design, organise or operate their services in such a way that can lead to excessive, impulsive or unwanted spending. That obligation shall include not exposing minors to variable reward systems including when purchased are carried

out with virtual currencies purchasable with funds within the meaning of Article 4, point (25) of Directive (EU) 2015/2366.

SECTION III – Obligations for AI companions and general conversational chatbots

Article 14 – Obligations for AI companions and general conversational chatbots

1. Providers of AI companions and of general conversational chatbots shall put in place proportionate and effective measures to ensure a high level of protection of the health, safety, fundamental rights and the well-being and development of minors that may access their AI system. Those measures shall include at least the following:

   (a) ensuring that minors are not exposed to addictive designs, by avoiding design features and system behaviours that simulate interpersonal relations that are likely to create emotional dependencies and by applying the measures set out in Article 9(1) and (3) to such systems;

   (b) ensuring that minors are provided with safe settings, by applying the measures set out in Article 11 to such systems, including by ensuring that, by default, their system does not use information or analysis derived from a minor's prior interactions in subsequent interactions, except where necessary to protect the minor's safety, to give effect to the settings referred to in Article 11;

   (c) ensuring transparency on economic transactions, by applying the measures set out in Article 13 to such systems;

   (d) ensuring that access to services and systems referred to in paragraph 1 for minors below the age of 13 years is only enabled and controlled by means of the tools for guardians referred to in Article 20;

   (e) performing state-of-the art evaluations and testing of the system for risks to the health, safety and fundamental rights and the physical, mental and emotional well-being and development of minors that are likely to arise when minors interact with the system, and implementing appropriate safeguards to address those risks, prior to the system’s placement on the market or putting into service;

   (f) post-market monitoring to identify, assess and, where appropriate, mitigate harms and emerging risks referred to in point (d) of this paragraph, including through detecting and responding to serious incidents involving minors, unless the system is provided by a micro or small enterprise within the meaning of Recommendation 2003/361/EC.

2. Where an AI companion or a general conversational chatbot is deployed as a functionality of an online social networking services, video-sharing platform services, or an online game in the provision of any such service, providers of such services shall ensure that:

   (a) the AI companion or general conversational chatbot is not activated automatically and, that the functionality is not displayed prominently on the online interface of that service;

   (b) minors are not encouraged to use the AI companion or general conversational chatbot;

   (c) where enabled, minors have the option to opt out easily and at any time, of using the AI companion or general conversational chatbot.

3. Providers of AI companions and of general conversational chatbots that adhere to a code of conduct assessed as adequate by the Commission in accordance with Article 23 may rely upon that code to demonstrate compliance with the obligations set out in this Article.

SECTION IV – Obligations for providers of online games

Article 15 – Obligations for providers of online games

1. Providers of online games shall put in place measures to ensure a high level of privacy, safety and security of minors. Those measures shall include at least the following:

   (a) ensuring that compulsive or excessive use of the game by minors is not encouraged, by applying Article 9(1) and Article 9(2), points (b) and (d);

   (b) ensuring settings of minors are set to a high level of privacy, security and safety, by applying Article 11(1);

   (c) ensuring contacts between minors and other recipients of the game are subject to a high level of privacy, security and safety, by applying Article 12(1) and 12(3), points (c);

   (d) ensuring mandatory access to the tools for guardians referred to in Article 20 and ensuring that access to services referred to in paragraph 1 for minors below the age of 13 years is only enabled and controlled by means of the tools for guardians referred to in Article 20.

2. Providers of online games shall put in place safeguards to prevent the game from being used to entice minors to initiate contacts on other services which may pose a risk to their privacy, safety and security.

3. Where providers of video gaming platforms provide recipients of the service with the possibility to create and upload video games on the service itself, such video gaming platforms shall put in place the necessary software and organisational measures to allow compliance of such video games with paragraphs 1 and 2 and Article 18 and Article 20.

4. Providers of online games that adhere to a code of conduct assessed as adequate by the Commission in accordance with Article 17 may rely upon such adherence to demonstrate compliance with the obligations set out in this Article.

SECTION V – Obligations for age-appropriate access

Article 16 – Obligations for providers of software application stores

1. Providers of software application stores shall put in place an age-rating system to allow to establish the age-appropriateness of software applications disseminated through their service. Such an age-rating system shall apply to each software application offered on the software application store and shall take due consideration of the evolving capacities of a minor.

2. Providers of software application stores shall not allow minors to access or purchase software applications that are inappropriate for their respective age in accordance with the age rating system established pursuant to paragraph 1 of this Article. This

obligation shall not affect the obligation of providers of services offered through software applications falling within the scope of Article 6.

3. Where the provider of a software application store becomes aware of software applications disseminated through its service that are subject to, or primarily consist of content that is subject to a higher minimum age under applicable Union law or national law in compliance with Union law than the one established in accordance with paragraph 1, the provider shall not allow minors below that higher minimum age from the Member State or States concerned to access or purchase such software applications.

4. In order to comply with paragraphs 2 and 3, providers of software applications stores shall assess the age of the recipient of the service, in accordance with Chapter V, including by means of the use of tools for guardians referred to in Article 20. Providers of software applications stores shall ensure that access to services referred to in paragraph 1 for minors below the age of 13 years is only enabled and controlled by means of the tools for guardians referred to in Article 20.

5. Providers of software application stores shall make publicly available information describing, in clear and accessible terms, the methodology, criteria and sources used for their age-rating systems.

6. Providers of software application stores shall allow the EU age verification solution using an EU proof of age attestation, certified as conforming with the EU Age Verification Scheme and included in the respective EU lists referred to in Article 30(1), to be offered in their store.

Article 17 – Codes of Conduct on age rating and online games

1. The Commission shall encourage and facilitate the drawing up of codes of conduct at Union level by [same day and month as the date of entry into application plus one year] with the involvement of providers of software application stores and online games, developers and providers of digital content, including software applications and online games, providers of age classification systems, organisations representing minors and their guardians, civil society organisations specialising in the protection of minors online as well as relevant authorities. The codes of conduct shall contribute to the harmonised establishing and application of age-rating systems including those referred to in Article 16(1), in particular by setting out common criteria and methodologies for such systems, and to the effective application of Article 15 with regard to online games.

2. The Commission shall aim to ensure that the codes of conduct address at least the following:

   (a) pursue the clearly defined and unambiguous objective to enable and facilitate the mutual recognition and consistent application of age ratings by providers of software application stores and online games across Member States;

   (b) define appropriate criteria, methodologies and sources of information for assessing the age-appropriateness of content in particular as regards violent, sexual, gambling and self-harm content as well as in-app purchases, contact risks and addictive design features;

   (c) establish free of charge remedies and redress mechanisms for content providers, including app developers to resolve disputes related to the age-rating

of content provided by a body that is impartial and independent, including financially independent, of providers and recipients of the service;

(d) provide harmonised, easily recognisable and understandable age-rating labels and textual descriptors to be displayed prominently and prior to accessing or purchasing content;

(e) provide for regular, transparent and independent monitoring and evaluation of the achievement of the objectives, including by containing key performance indicators to measure the achievement of their objectives and regular updates to reflect technological developments and emerging risks to minors;

(f) with regard to online games, define appropriate measures and methodologies to give effect to the obligations laid down in Article 15(1), (2), (3) and (4), building, where appropriate, on existing pan-European age classification frameworks, including their criteria concerning interactive functionalities and monetisation practices, and providing for their regular update in light of scientific and technological developments and emerging risks to minors

3. By [same day as date of entry into force plus 42 months] the Commission shall assess whether the codes of conduct meet the aims specified in paragraph 2 and and are adequate to demonstrate compliance with the respective obligations. The Commission shall regularly monitor and evaluate the achievement of their objectives, having regard to the key performance indicators that they might contain and shall publish its assessment. Where the Commission assesses adherence to point (f) of paragraph 2, Article 15(4) shall apply.

SECTION VI – General obligations on agency of minors and empowering tools for minors and guardians

Article 18 - Agency of minors

1. Providers of online social networking services, of video-sharing platform services, of online games, of AI companions, and of general conversational chatbots, shall ensure that the features, communication, information, user-control tools and mechanisms of the service and the system, warnings, and any other information referred to in Chapter III are easily accessible to all minors and presented in a way that minors can understand. Where a provider is a provider of a very large online platforms designated in accordance with Article 33 of Regulation (EU) 2022/2065, that provider shall ensure that information referred to in this paragraph is made available in the official language(s) of the Member State(s) in which the service is provided.

2. Providers referred to in paragraph 1 shall put in place the following:

(a) tools that allow minors to control and provide feedback on content, prompts, information suggested and search results to which they are exposed and that have immediate and durable effects on such content, prompts, information suggested and search results;

(b) mechanisms that allow minors to control the settings which determine how they interact and communicate with, transfer, create or generate content on the service or the system, including warning signals, and explanations, that allow for temporary changes and that ensure that minors can easily return to previous or default settings.

Article 19 – Child-friendly reporting and support tools for minors

1. Providers of online social networking services, of video-sharing platform services, of video gaming platforms, of AI companions, and of general conversational chatbots shall put in place mechanisms that allow minors to report content, accounts, groups, features or behaviour, as applicable, which they consider harmful to their privacy, safety, or security. Such mechanisms shall be easy to access and designed in a way that minors can understand. Where a provider is a provider of a very large online platform designated in accordance with Article 33 of Regulation (EU) 2022/2065, that provider shall ensure that those mechanisms are made available in the official language(s) of the Member State(s) in which the service is provided.

2. Where a provider referred to in paragraph 1 is an online platform subject to Article 17 of Regulation (EU) 2022/2065, any restrictions imposed following reports referred to in paragraph 1 of this Article shall be considered as a restriction of the visibility pursuant to Article 17(1), point (a) of Regulation (EU) 2022/2065.

3. Providers referred to in paragraph 1 shall take the necessary technical and organisational measures to ensure that reports submitted by minors in accordance with paragraph 1 are processed and addressed as a priority and without undue delay and that minors receive information about the procedure undertaken and the possibilities of redress.

4. Providers referred to in paragraph 1, shall:

   (a) ensure that minors have access to support and authoritative information sources when encountering illegal or harmful content on the service or system, including by informing minors of available resources and organisations at national and Union level;

   (b) ensure that support and authoritative information sources referred to in point (a) of this paragraph are presented to minors where necessary, and at least after minors have submitted a report pursuant to paragraph 1;

   (c) make reasonable efforts to display clear warning messages where minors are likely to publish or to be exposed to content or interactions presenting a risk to their privacy, safety or security.

Article 20 – Tools for guardians

1. Providers of online social networking services, of video-sharing platform services, of online games, of AI companions, and of general conversational chatbots shall implement effective, accessible and user-friendly tools for guardians that meet at least the following conditions:

   (a) they are tailored to the age of the minor, taking due account of the minor's gradual development;

   (b) they are easy to use, access and activate for minors and guardians;

   (c) they ensure that changes can only be made with the same degree of authorisation that is required for the initial activation of the tools;

   (d) they are effective and cannot be easily circumvented or undermined by the design or operation of the service or the system.

   (e) they do not disproportionately restricting minors' rights;

(f) they respect minor's agency and privacy.

2. Providers referred to in paragraph 1 shall ensure minors are informed when any tool for guardians referred to in paragraph 1 is being used.

3. Providers referred to in paragraph 1 shall encourage guardians to use the tools referred to in that paragraph and shall regularly remind them of their availability and objectives and of the need to update them. This shall include displaying clear warning messaging on managing the settings of minors.

4. Providers referred to in paragraph 1 shall integrate the following mechanisms into the tools for guardians referred to in that paragraph:

(a) effective measures to ensure time-limited access pursuant to Article 9(3), Article 14(1), point (b) and Article 15(1), point (b);

(b) mechanisms aimed at managing settings pursuant to Articles 11 and 12;

(c) mechanisms aimed at enabling guardians, on behalf of minors, to report content, accounts, groups or behaviour which they consider harmful to the privacy, safety, or security of minors pursuant to Article 19(1).

5. Providers of very large online platforms designated in accordance with Article 33 of Regulation (EU) 2022/2065 shall ensure that the tools for guardians referred to in paragraph 1 are interoperable with tools for guardians provided by third parties, in accordance with the conditions set out in Article 6 of Regulation (EU) 2022/1925, where relevant.

6. Providers referred to in paragraph 1 shall ensure guardians and minors are able to report, pursuant to Article 19, where tools for guardians referred to in paragraph 1 are not operational and do not function as prescribed.

7. The Commission shall be empowered to adopt delegated acts in accordance with Article 40 to supplement this Regulation by laying down the technical and operational requirements for the tools for guardians referred to in paragraph 1 of this Article.

Article 21 – Collective complaints

1. Without prejudice to Article 86 of Regulation (EU) 2022/2065 and to Directive (EU) 2020/1828 or to any other type of rules on representation under national law, minors and guardians who are recipients of online social networking services, of video-sharing platform services, of video gaming platforms, and users of AI companions or of general conversational chatbots, shall at least have the right to mandate a body, organisation or association to exercise the rights conferred by this Regulation on the minors' behalf, provided that the body, organisation or association meets all of the following conditions:

(a) it operates on a not-for-profit basis;

(b) it has been properly constituted in accordance with the law of a Member State;

(c) its statutory objectives include a legitimate interest in ensuring that this Regulation is complied with.

2. In addition to the right to lodge a complaint in accordance with Article 53 of Regulation (EU) 2022/2065, minors and guardians who are recipients of online social networking services, of video-sharing platform services, of video gaming

platforms, and users of AI companions and general conversational chatbots, and any body, organisation or association referred to in paragraph 1 of this Article shall have the right to lodge a complaint alleging an infringement of this Regulation against providers of the aforementioned services and systems with the competent authority determined in accordance with Article 34 of the Member State where the recipient of the service or the user of the system is located or established, or with the European AI Office for AI companions or the general conversational chatbots falling under its exclusive competence pursuant to Article 75(1) of Regulation (EU) 2024/1689.

SECTION VII – Other due diligence obligations for a safe online environment

Article 22– Monitoring obligation for providers of very large online platforms

1. Providers of services referred to in Article 8(1) of this Regulation that have been designated as very large online platforms in accordance with Article 33 of Regulation (EU) 2022/2065 shall monitor, test and evaluate the effectiveness of the measures implemented in accordance with this Chapter.

2. The assessment referred to in paragraph 1 of this Article shall be part of the risk assessment carried out pursuant to Article 34 of Regulation (EU) 2022/2065.

Article 23 - Codes of conduct

1. The Commission shall encourage and facilitate the drawing up of voluntary codes of conduct at Union level to contribute to the proper application of this Regulation. The Commission shall invite providers of relevant services and systems in scope, relevant national competent authorities, civil society organisations, industry, academia, parents, educators and other relevant stakeholders to participate in the drawing-up of those codes of conduct.

2. When giving effect to paragraph 1, the Commission shall aim to ensure that the codes of conduct clearly set out their specific objectives, contain commitments to take specific measures to achieve those objectives, and take due account of the specificities of different services and systems provided, and the needs and interests of all interested parties, in particular minors, at Union level. The Commission shall also aim to ensure that participants report regularly to the Commission and their respective competent authorities under this Regulation. The reporting commitments sought by the Commission shall take into account differences in size and capacity between different providers.

3. The Commission, after consultation of the European Digital Services Board or the European Artificial Intelligence Board for aspects of codes within the remit of their competence, shall assess whether codes of conducts meet the aims specified in paragraphs 1 and 3 and are adequate to demonstrate compliance with the respective obligations set out in this Regulation. The Commission shall publish that assessment. It shall regularly monitor and evaluate the achievement of the objectives of the codes of conduct and, after consultation of the European Digital Services Board or the European Artificial Intelligence Board, shall update the assessment as appropriate.

4. The Commission shall encourage and facilitate regular review and adaptation of the codes of conduct.

5. The Commission shall also encourage developments of best practices in any area falling within the scope of this Regulation. This may include areas such as testing in

the course of product developments or control standards. The is without prejudice to Article 5.

Article 24 - Legal representatives

1. Providers of online social networking services, of video-sharing platform services, of online games, of AI companions, and of general conversational chatbots, which do not have an establishment in the Union but which offer services or systems in the Union, shall designate, in writing, a legal or natural person to act as their legal representative in one of the Member States where the provider offers its services or system. However, where such providers have already designated a legal representative pursuant to Article 13 of Regulation (EU) 2022/2065 or pursuant to Article 22 or Article 54 of Regulation (EU) 2024/1689, they may extend the mandate of that legal or natural person to all issues necessary for the receipt of, compliance with and enforcement of decisions issued in relation to this Regulation.

2. Article 13(2) to (5) of Regulation (EU) 2022/2065 shall apply and references to Regulation (EU) 2022/2065 shall be construed as references to this Regulation with regard to obligations set out in this Regulation in relation to providers of online social networking services, of video-sharing platform services, and of online games. Article 22(2), (3) and (4) of Regulation (EU) 2024/1689 or Article 54 (2) to (5) of that Regulation shall apply and references to obligations set out in Regulation (EU) 2024/1689 shall be construed as references to this Regulation with regard to obligations set out in this Regulation in relation to providers of AI companions and of general conversational chatbots.

Article 25 – Amendments to listed measures

1. The Commission may adopt delegated acts in accordance with Article 40 for the purpose of amending Articles 9(2), 10(2), 11(1), 12(1), 12(2), 14(1), 15(1) and 18(2), for providers of online social networking services, of video-sharing platform services, of online games, of AI companions, and of general conversational chatbots, to ensure a high-level of privacy, safety and security of minors on their service or system. Those delegated acts shall be based on identified emerging risks which undermine the health and well-being, as well as the privacy, safety and security of minors leading to the need to keep the following obligations up to date in order to ensure effective compliance with these obligations:

   (a) prohibitions on practices intended, or which can reasonably be foreseen, to encourage compulsive or excessive use of the service by minors, as referred to in Article 9(2);

   (b) measures ensuring that recommender systems are designed in way that ensures a high level of privacy, safety and security of minors, as referred to in Article 10(2);

   (c) default settings ensuring that minors' accounts are set to a high level of privacy, safety and security, as referred to in Article 11(1);

   (d) measures ensuring a high level of privacy, safety and security of minors as regards contacts between minors and other recipients of the service, as referred to in Article 12(1) and measures limiting the visibility of any information shared by minors and their interactions with other recipients of the service, as referred to in Article 12(2)

(e) measures ensuring a high level of protection of health, safety, fundamental rights and well-being of minors that may access AI companions and general conversational chatbot systems, as referred to in Article 14(1);

(f) measures ensuring a high level of privacy, safety and security of minors on online games as referred to in Article 15(1);

(g) measures ensuring agency for minors as referred to in Article 18(2).

2. When considering the adoption of a delegated act, the Commission shall take into account:

(a) the extent to which the risk has already caused harm to minors' health, well-being or had adverse impact on minors' privacy, safety and security, or fundamental rights or has given rise to significant concerns in relation to the likelihood of such harm or adverse impact, as demonstrated, for example, by reports or documented allegations submitted to national competent authorities or by other reports, as appropriate;

(b) the potential extent of such harm or such adverse impact, in particular in terms of its intensity and its ability to affect multiple persons or to disproportionately affect a particular group or persons;

(c) the impact of the existing measures in addressing such risks, including the intended purpose of such measures, the extent to which the measures are being used or are likely to be used, and the effectiveness of such measures for minors' health, well-being, and privacy, safety and security.

CHAPTER IV – VERIFICATION OF PARENTAL RESPONSIBILITY

Article 26 - Verification of parental responsibility

1. For the purpose of creating an account with limited features pursuant to Article 6(2) or age-appropriate experience on video-sharing platforms pursuant to Article 7(2) and for the purpose of implementing effective, accessible and user-friendly tools for guardians pursuant to Article 20(1), a provider of a service referred in those provisions shall be able to:

(a) use signals of the parental responsibility based on freely accessible official online databases or online interfaces made available by a Member State;

(b) use signals of the parental responsibility that the provider may already be in possession of in view of the past engagements of the respective minor and adult with parental responsibility with the service concerned;

(c) accept self-declaration by the adult with the parental responsibility at least until the delegated act as referred to in paragraph 3 is adopted.

2. When using signals referred to in paragraph 1, point (a), the provider shall make reasonable efforts to verify that the information available is reliable and complete.

3. When using self-declarations referred to in paragraph 1, point (c), the provider shall make reasonable efforts to verify that the adult making the self-declaration is exercising parental responsibility.

4. Verification of the parental responsibility pursuant to paragraph 1 shall be carried out in a privacy-preserving manner and shall not lead to additional processing of

personal data that could enable the provider to determine the location of the adult or minor concerned or to track, target or profile the adult or minor.

5. The Commission is empowered to adopt a delegated act in accordance with Article 39 to supplement this Regulation by specifying signals indicating parental responsibility pursuant to paragraph 1, point a of this Article.

CHAPTER V – AGE ASSURANCE

Section I – General principles for age assurance

Article 27 – General principles for age assurance

Where providers of services and of systems subject to Chapters II and III implement age assurance solutions in order to fulfil their obligations laid down in this Regulation, they shall ensure that those solutions provide a high level of accuracy, reliability, security, robustness, non-intrusiveness, privacy and data protection, and non-discrimination.

Article 28 – Data protection in age assurance

1. Age assurance solutions shall not enable the identification of the recipient nor locate, track, target, advertise to or profile recipients for any purpose.

2. Providers of services and of systems falling within the scope of this Regulation, and any entity acting on behalf or together with such providers in age assurance, shall not maintain, acquire or process more personal data than strictly necessary to assess if the recipient of the service or the user of the system has met the age thresholds laid down in this Regulation, and shall not further process, share or combine this information with any additional data, without prejudice to Article 29(6), and they shall not combine personal data stored or relating to the use of the system with personal data from any other services offered by the provider or from third-party services.

3. Providers of services and of systems falling within the scope of this Regulation, and any entity acting on behalf or together with such providers in age assurance, shall ensure that the measures used are based on state-of-the-art technology. Any age assurance measure shall be zero knowledge proof.

4. By way of derogation from paragraph2, providers referred to in Article 16(4) and Article 8(1) may store, at account level, the age signal that a user has successfully met a specific age threshold under this Regulation, for the sole purpose of avoiding repeated age assurance. Such age signal shall be limited to the minimum information necessary for that purpose.

5. Providers of services and of systems falling within the scope of this Regulation shall take the necessary technical and organisational measures to comply with paragraphs 1, 2, 3 and 4.

Section II – Specific obligations on age assurance

Article 29 – Age assurance solutions

1. Providers of services referred to in Article 6 of this Regulation shall put in place age verification solutions to verify, under the conditions set out in this Chapter, whether the recipient of the service has reached the minimum age pursuant to those provisions, or, where applicable, whether the creation of a parental account is necessary.

2. For the purpose of compliance with Article 6 providers referred to in that paragraph shall rely exclusively on an EU age verification solution using an EU proof of age attestation, provided by a third party, certified as conforming with the EU Age Verification Scheme and included in or verifiable against the respective EU lists referred to in Article 30, paragraph 1, point (a) and (b).

3. EU age verification solutions and EU proof of age attestations, shall be certified as conforming with the requirements of the EU Age Verification Scheme, as laid down in accordance with Article 30(2), by a public authority. European Digital Identity Wallets certified pursuant to Article 5c of Regulation (EU) No 910/2014 that comply with the requirements of the EU Age Verification Scheme shall be deemed to be certified in accordance with this paragraph. Providers of EU proof of age attestations and providers of EU age verification solutions shall comply with the requirements of the EU Age Verification Scheme.

4. For the purpose of complying with the obligations of Article 8(1) and Article 16(2) and 16(3), the providers concerned may use age assurance solutions other than the EU age verification solutions referred to in paragraph 2, where they can demonstrate that those solutions meet the requirements laid down in Article 27 and Article 28.

5. Providers of services and of systems referred to in paragraphs 1 and 4 shall ensure that recipients have access to an effective internal complaint-handling mechanism enabling them to lodge, by electronic means and free of charge, complaints against the outcome of the age assurance referred to in those paragraphs, where the recipient considers the outcome of the age assurance to be incorrect. Providers of online platforms, as defined in Article 3 point (i) of Regulation 2022/2065 may for the purpose of compliance with this Article use the complaint-handling mechanism laid down in Article 20 of that Regulation 2022/2065.

6. Where a provider of an operating system has obtained an age signal of a user, and where the age assurance used to obtain this age signal is in compliance with the requirements defined pursuant to Article 27, after obtaining consent of the user, the provider of an operating system shall enable the sharing of the age signal with providers in scope when such age signal of a user is required to comply with this Regulation.

Article 30 - Empowerment to the Commission

1. The Commission shall maintain:

   (a) an EU list of providers of EU proof of age attestations certified in accordance with Article 29(2) and notified by any Member State;

   (b) an EU list of EU age verification solutions certified in accordance with Article 29(2) and notified by any Member State.

   The Commission shall publish the EU list and keep it up to date in a secure and machine-readable form.

2. The Commission shall adopt implementing acts laying down the specifications as a basis of the functioning of the EU Age Verification Scheme, including the requirements applicable to EU age verification solutions and to the issuance, presentation and verification of EU proof of age attestations. Such implementing acts shall be limited to what is necessary to ensure the effective, secure, privacy-preserving, interoperable and uniform implementation of Article 29(2) and (3) and shall be based on the principle of data minimisation, purpose limitation, security, technological neutrality and proportionality, and shall ensure interoperability with the European Digital Identity Wallets provided pursuant to Article 5a of Regulation (EU) No 910/2014. Those implementing acts shall specify the detailed technical, organisational, privacy and security requirements applicable to EU proof of age attestations and their providers and for EU age verification solutions and their providers, the evidence and procedures for demonstrating and assessing public authorities, and the specifications of the EU lists referred to in paragraph 1. The implementing acts may also include requirements for a trust mark for age verification solutions. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 40(2).

3. The Commission shall adopt delegated acts, in accordance with Article 39, in order to supplement this regulation by specifying:

   (a) the requirements applicable to alternative age assurance solutions as referred to in Article 29(4), including the requirements necessary to demonstrate compliance with Article 27 and Article 28. Those delegated acts shall specify the detailed technical, organisational, privacy and security requirements applicable;

   (b) the obligations applicable to operating systems as referred to in Article 29(6), including the requirements necessary to ensure the secure, privacy-preserving and interoperable sharing of age signals.

Article 31 – Obligations on Member States

1. Member States shall 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, for the purposes of Article 26(1), point (a), and of the exercise of the tools for guardians referred to in Article 20. Such means shall be:

   (a) be based on authentic sources established under national law;

   (b) be free of charge for the guardian;

   (c) not entail making any information on parental responsibility accessible to providers or to the public beyond the confirmation that parental responsibility exists.

2. Member States shall ensure that privacy-preserving electronic means referred to in paragraph 1 are effectively accessible to all citizens and guardians and minors residing in their territory, including persons with disabilities, persons with limited digital access or skills, and persons in vulnerable situations such as refugee and displaced families.

3. Member States shall provide for appropriate alternative procedures where parental responsibility cannot be demonstrated through standard civil status documentation.

4. Member States shall take the necessary measures to ensure the availability of means of obtaining a proof of age attestation to verify the minimum age set out in this Regulation.

5. Member States shall take the necessary measures to ensure the availability for citizens and residents, free of charge, of at least one EU age verification solution as certified in accordance with Article 29(3) to verify the age thresholds set out in this Regulation.

6. Member States shall ensure that public authorities can be accredited for the purposes of Article 29(3) and shall communicate to the Commission the names and addresses of the public authorities designated and accredited in their territory, as well as any subsequent changes thereto. The Commission shall make that information publicly available.

7. Member States shall notify to the Commission, without undue delay, the EU age verification solutions and EU proof of age attestations certified in accordance with Article 29(3), together with the corresponding certificate of conformity, as well as any subsequent suspension or withdrawal of a certificate. Once included in the lists referred to in Article 29(1) point (a) and (b), an EU age verification solution and EU proof of age attestations shall be recognised by all Member States for the purposes of this Regulation.

Article 32 – Existing accounts

1. For the purposes of establishing, in accordance with Article 6(4), whether an existing account belongs to a recipient below the age of 15 years, providers referred to in Article 6(1) shall rely on an age verification solution referred to in Article 30(2).

2. By way of derogation from paragraph 1 of this Article, providers referred to in that paragraph shall not be required to carry out age verification where they can establish, with a high degree of confidence, that the recipient of the service has reached the minimum age set out in Article 6.

3. By way of derogation from Article 8(1), providers falling within the scope of that Article and providers of software application stores shall not be required to assess the age of the recipient where they can establish, with a high degree of confidence that the recipient of the services is not a minor.

4. Providers of very large online platforms designated in accordance with Article 33 of Regulation (EU) 2022/2065 that fall within the scope of this Article, shall submit a plan to the competent authority specifying how they intend to comply with paragraph 1 and Article 8(1) and, in case they intend to rely on the exceptions laid down in paragraphs 2 and 3, how they intend to establish that the recipient of the service or the user of the system has reached the minimum age, in accordance with those paragraphs.

CHAPTER VI – MEASURES TO SUPPORT MINORS

Article 33 – National measures to prepare and support minors

1. Member States shall support the protection of minors by establishing national strategies to ensure that minors and their guardians have the following:

(a) easy, free and confidential access at national level to channels through which minors can seek assistance in relation to the harms addressed by this Regulation, including unwanted contact and cyberbullying;

(b) adequate information about the risks addressed by this Regulation and of the available means of protection, including by addressing digital literacy;

(c) other information relevant to protect minors online.

2. Member States' activities to support the protection of minors shall build on the experience and expertise of the Safer Internet Centres with their awareness raising activities, their helplines supporting children, guardians and educators, and their hotlines to report suspected illegal content.

3. Member States shall communicate the strategies referred to in paragraph 1 to the Commission by [same day as the date of entry into force plus 12 months].

4. The activities referred to in paragraph 1 may be supported by Union funding made available under the relevant Union programmes and instruments established under the multiannual financial framework.

5. The Commission shall facilitate the exchange of best practices between Member States, including on the development of digital literacy skills, and on the establishment and operation of national support channels and applications.

CHAPTER VII – COMPETENCES, SUPERVISION AND ENFORCEMENT

Article 34 – Competences, Supervision and Enforcement

1. For the purposes of the supervision and enforcement of obligations imposed by this Regulation on providers of online social networking services, of video-sharing platform services, of online games that are video gaming platforms, and of software application stores, Chapter IV of Regulation (EU) 2022/2065 shall apply and any references therein to the provider of intermediary services shall be construed to include the provider of services covered by this Regulation. Any references therein to compliance or non-compliance with the relevant provisions of Regulation (EU) 2022/2065 shall be deemed to include this Regulation.

2. For the purposes of the supervision and enforcement of obligations imposed by this Regulation on providers of AI companions and of general conversational chatbots, Chapter IX of Regulation (EU) 2024/1689 shall apply, and any references therein to compliance or non-compliance with the relevant provisions of Regulation (EU) 2024/1689 shall be construed to include Chapters II, III and IV of this Regulation. Non-compliance with those obligations shall be subject to administrative fines under Article 99 of Regulation (EU) 2024/1689 not exceeding 6 % of the total worldwide annual turnover of the undertaking providing the AI companion or the general conversational chatbot in the preceding financial year where that provider has been found to have acted intentionally or negligently.

3. Member States shall ensure that authorities designated by them in accordance with Article 49 of Regulation (EU) 2022/2065 and Articles 70 and 74 of Regulation (EU) 2024/1689 are competent to supervise and enforce this Regulation in respect of providers of services or systems covered by this Regulation.

4. To the extent that powers are conferred on the Commission under Section 4 of Chapter IV of Regulation (EU) 2022/2065 and under Article 75a to 75d and Article

99 of Regulation (EU) 2024/1689, those powers shall also cover the supervision, investigation, enforcement and monitoring of compliance with this Regulation.

5. Member States shall ensure that a competent authority is responsible for the supervision of providers of online games that are video games and for the enforcement of Article 15 and applicable provisions in Articles 8 and 18 to 22. Such competent authority shall have the powers set out in Article 51 of Regulation (EU) 2022/2065. For the purpose of this paragraph, Member States shall lay down rules on penalties applicable to infringements of Article 15 and applicable provisions in Articles 8 and 18 to 22 as set out in Article 52 of Regulation (EU) 2022/2065. The competent authority of the Member State in which the main establishment of the provider of online games that are video games is located shall have exclusive powers to supervise and enforce this Regulation.

6. The supervisory authorities referred to in Article 51 of Regulation (EU) 2016/679 shall be competent to monitor the processing of personal data necessary to comply with this Regulation, and in particular Articles 27, 28 and 29 of this Regulation. For infringements of the data protection obligations laid down in those Articles, the data protection supervisory authorities may within their competence impose fines in line with Article 83 of Regulation (EU) 2016/679 and up to the amount referred to in Article 83(5) of that Regulation.

7. Member State authorities shall not take decisions which run counter to a decision adopted by the Commission under this Regulation. The Commission and the Member States, including Digital Services Coordinators, market surveillance authorities and national authorities responsible for the enforcement of consumer protection laws, shall work in close cooperation and coordination.

Article 35 - Expedited procedure

1. For the purposes of Section 4 of Chapter IV of Regulation (EU) 2022/2065 and Chapter IX of Regulation (EU) 2024/1689, where the obligations in this Regulation apply to providers of very large online platforms designated in accordance with Article 33 of Regulation (EU) 2022/2065 or to providers of AI systems under the exclusive supervision of the Commission in accordance with Regulation (EU) 2024/1689, the powers conferred upon the Commission under Chapter IV of Regulation (EU) 2022/2065 and Chapter IX of Regulation (EU) 2024/1689 shall be exercised in accordance with this Article.

2. Where the Commission initiates proceedings for infringement of this Regulation in accordance with Article 66 of Regulation (EU) 2022/2065 or Article 75a of Regulation (EU) 2024/1689 in view of the possible adoption of decisions pursuant to Articles 73 and 74 of Regulation (EU) 2022/2065 or Articles 75c of Regulation (EU) 2024/1689, the Commission shall endeavour to:

   (a) communicate its preliminary findings to the provider concerned within [30] working days from the opening of the proceedings pursuant to Article 66 of Regulation (EU) 2022/2065 or Article 75a of Regulation (EU) 2024/1689;

   (b) adopt a final decision within 90 working days from the opening of proceedings.

Article 36 – Supervisory fee

1. The Commission shall charge an annual supervisory fee on providers of very large online platforms designated in accordance with Article 33 of Regulation (EU) 2022/2065 which constitute, are embedded in or embed online social networking services, video-sharing platform services, or software application stores, and on providers of AI companions, general conversational chatbots, and video gaming platforms for which it enjoys the competence to supervise their compliance with Chapters II to V of this Regulation in accordance with Article 33 of this Regulation.

2. Each provider referred to in paragraph 1 shall be charged the annual supervisory fee for each service or system falling within the scope of this Regulation.

3. The overall amount of the annual supervisory fees pursuant to paragraph 1 shall cover the costs incurred by the Commission in the preceding calendar year in relation to its supervisory tasks under this Regulation vis-à-vis the providers referred to in paragraph 1, in particular costs related to human resources, including officials, the set-up, maintenance and operation of the EU Age Verification Scheme pursuant to Article 29, the exercise of supervisory and enforcement tasks pursuant to Article 34, and the development of expertise and capabilities pursuant to Article 37.

4. For the purpose of establishing the annual supervisory fee for the tasks pursuant to paragraph 3, the annual supervisory fee for each of the providers referred to in paragraph 1 shall not exceed 0,03 % of its worldwide annual net income in the preceding financial year.

5. For the purpose of the application of this Article, the Commission shall apply rules and principles laid down in Article 43 of Regulation (EU) 2022/2065.

6. The Commission shall adopt delegated acts, in accordance with Article X, laying down the detailed methodology and procedures for:

   (a) the determination of the estimated costs referred to in paragraph 3;

   (b) the determination of the individual annual supervisory fees referred to in paragraph 1;

   (c) the determination of the maximum overall limit defined in paragraph 4; and

   (d) the detailed arrangements necessary to make payments.

   When adopting those delegated acts, the Commission shall respect the principles set out in paragraph 5 of this Article.

Article 37 – Development of expertise and capabilities

The Commission, in cooperation with the competent authorities pursuant to Article 34, shall develop Union expertise and capabilities in the area of protection of minors, including, where appropriate, through the secondment of Member States' personnel. Such development of expertise and capabilities shall especially be developed in the area of incidents affecting the protection of minors.

Article 38 – Incidents reaction mechanisms

1. The Commission, in cooperation with the competent authorities pursuant to Article 33, shall coordinate the assessment of incidents affecting the protection of minors across the Union in relation to services and systems in scope, and be able to rely on

the expertise and resources of such authorities. Member States shall cooperate with the Commission in setting up efficient knowledge sharing networks with other authorities and relevant third parties.

2. The Commission shall establish a voluntary administrative arrangement with competent authorities setting out procedures to facilitate a rapid response in the event of an incident affecting the protection of minors in the Union or in significant parts of it. Member States shall establish minimum preparedness levels for national authorities to ensure regular communications channels between relevant national authorities and third parties, and map existing incident reaction protocols at national level and where relevant establish new ones. The incident reaction mechanism shall complement the existing crisis tools under Regulation (EU) 2022/2065 and inform their potential activation.

CHAPTER VIII - IMPLEMENTING AND DELEGATED ACTS

Article 39 – Exercise of the delegation

1. The power to adopt delegated acts is conferred upon the Commission subject to the conditions laid down in this Article.

2. The delegation of power referred to in Articles 2(5), 6(6), 7(6), 20(7), 25(1), 26(3), 30(3) and 36(6) shall be conferred on the Commission for a period of five years from [same day as date of entry into force]. The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the five-year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.

3. The delegation of power referred to in Articles 2(5), 6(6), 7(6), 20(7), 25(1), 26(3), 30(3) and 36(6) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.

5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

6. A delegated act adopted pursuant to Articles Articles 2(5), 6(6), 7(6), 20(7), 25(1), 26(3), 30(3) and 36(6) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of two months of notification of that act to the European Parliament and to the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by three months at the initiative of the European Parliament or of the Council.

Article 40 – Committee procedure

1. The Commission shall be assisted by a committee ('the Child Safety Committee'). That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

3. Where the opinion of the committee is to be obtained by written procedure, that procedure shall be terminated without result when, within the time limit for delivery of the opinion, the chair of the committee so decides or a simple majority of committee members so request.

CHAPTER IX - FINAL PROVISIONS

Article 41 – Amendment to Directive (EU) 2020/1828

In Annex I to Directive (EU) 2020/1828, the following point is added: [final name of the act].

Article 42 - Review

1. The Commission shall review the application of this Regulation and shall report to the European Parliament and to the Council by [31 August 2030]. Taking into account the experience gained in the application of this Regulation, as well as technological, market and legal developments, the Commission shall evaluate in particular:

   (a) the contribution of this Regulation to the deepening and efficient functioning of the internal market and to ensuring a high level of protection for minors online in the European Union;

   (b) the effectiveness of the application of Articles 6 and 7;

   (c) the personal scope of the provisions in Chapters II and III;

   (d) the impact of this Regulation on the respect for the right to freedom of expression and information.

2. The report referred to in paragraph 1 shall be accompanied, where appropriate, by a proposal for amendment of this Regulation.

3. In addition, the Commission shall submit a report to the European Parliament and the Council every four years after the report referred to in paragraph 1 on the progress towards achieving the objectives of this Regulation.

Article 43 – Entry into force and application

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

This Regulation shall apply from [same day as entry into force plus 6 months].

However, Article 5 shall apply from [same day as entry into force] and Articles 33 and 35 shall apply from [same day as entry into force plus 12 months].

This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaties.

Done at Brussels,

For the European Parliament *The President*	*For the Council* *The President*

LEGISLATIVE FINANCIAL AND DIGITAL STATEMENT

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE 3
1.1. Title of the proposal/initiative 3
1.2. Policy area(s) concerned 3
1.3. Objective(s) 3
1.3.1. General objective(s) 3
1.3.2. Specific objective(s) 3
1.3.3. Expected result(s) and impact 4
1.3.4. Indicators of performance 4
1.4. The proposal/initiative relates to: 6
1.5. Grounds for the proposal/initiative 6
1.5.1. Requirement(s) to be met in the short or long term including a detailed timeline for roll-out of the implementation of the initiative 6
1.5.2. Added value of EU involvement (it may result from different factors, e.g. coordination gains, legal certainty, greater effectiveness or complementarities). For the purposes of this section 'added value of EU involvement' is the value resulting from EU action, that is additional to the value that would have been otherwise created by Member States alone. 7
1.5.3. Lessons learned from similar experiences in the past 7
1.5.4. Compatibility with the multiannual financial framework and possible synergies with other appropriate instruments 7
1.5.5. Assessment of the different available financing options, including scope for redeployment 8
1.6. Duration of the proposal/initiative and of its financial impact 9
1.7. Method(s) of budget implementation planned 9
2. MANAGEMENT MEASURES 10
2.1. Monitoring and reporting rules 10
2.2. Management and control system(s) 10
2.2.1. Justification of the budget implementation method(s), the funding implementation mechanism(s), the payment modalities and the control strategy proposed 10
2.2.2. Information concerning the risks identified and the internal control system(s) set up to mitigate them 12
2.2.3. Estimation and justification of the cost-effectiveness of the controls (ratio between the control costs and the value of the related funds managed), and assessment of the expected levels of risk of error (at payment & at closure) 12
2.3. Measures to prevent fraud and irregularities 12
3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE 14

3.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected 14
3.2. Estimated financial impact of the proposal on appropriations 15
3.2.1. Summary of estimated impact on operational appropriations 15
3.2.1.1. Appropriations from voted budget 15
3.2.1.2. Appropriations from external assigned revenues 15
3.2.2. Estimated output funded from operational appropriations 17
3.2.3. Summary of estimated impact on administrative appropriations 19
3.2.3.1. Appropriations from voted budget 19
3.2.3.2. Appropriations from external assigned revenues 19
3.2.3.3. Total appropriations 19
3.2.4. Estimated requirements of human resources 20
3.2.4.1. Financed from voted budget 20
3.2.4.2. Financed from external assigned revenues 20
3.2.4.3. Total requirements of human resources 21
3.2.5. Overview of estimated impact on digital technology-related investments 24
3.2.6. Compatibility with the current multiannual financial framework 25
3.2.7. Third-party contributions 25
3.3. Estimated impact on revenue 25
4. DIGITAL DIMENSIONS 26
4.1. Requirements of digital relevance 27
4.2. Data 27
4.3. Digital solutions 28
4.4. Interoperability assessment 28
4.5. Measures to support digital implementation 28

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

1.1. Title of the proposal/initiative

Child Online Safety and Rights Act (CARE)

1.2. Policy area(s) concerned

Policy area: Protecting minors online in the policy areas of communications networks, content and technology; public health; and internal market, industry, entrepreneurship and SMEs.

The budgetary impact concerns the new supervisory tasks entrusted to the Commission in relation to online social networking services, video-sharing platform services, software application stores as well as AI companions and general conversational chatbots within the Commission competence. Some limited impacts also arise from the new obligations on video games, although direct supervision lies with the Member State authorities.

1.3. Objective(s)

1.3.1. General objective(s)

This proposed Regulation follows up on the conclusions of the report by the Co-chairs of the Special Panel on Child Safety Online, which set out a clear path for how children in Europe can be better protected in the online environment.

As set out in the report, children spend an increasing amount of time online and, in doing so, are exposed to many different risks such as exposure to age-inappropriate content, cyberbullying, excessive time spent online, and unwanted contacts from strangers. These risks carry serious consequences for children's mental health and well-being, with adolescents and children being a particularly vulnerable group.

The EU market risks becoming increasingly fragmented as Member States are planning or adopting new measures to restrict access to certain online platforms considered risky for children below a specified age – with differences in scope, age limit and proposed restrictions – thereby creating legal uncertainty, high compliance costs for businesses and an unequal level of protection for minors in a digital environment that knows no borders.

To ensure a safe and age-appropriate digital environment for minors and as also noted in the report by the Co-chairs of the Special Panel, age assurance is critical for effectively protecting minors online. Age assurance underpins both age restrictions and safety measures of children. However, the current legal framework around age assurance lacks clarity and its implementation is patchy.

Against this background, this proposed Regulation aims at ensuring a **strong and coherent framework for the protection of minors online**, taking the child and their empowerment and fundamental rights as a starting point.

1.3.2. Specific objective(s)

Taking into account the general objective to protect minors online, the proposal pursues the following specific objectives:

Delay minors' access to to services with specific features that constitute social network services or video-sharing platforms. For these services, shall not allow

minors below the age of 15 to create an account. Providers of those services may allow guardians to set up accounts for minors above the age of 13 with limited features to access the service. Where such providers can demonstrate that they are a child-friendly service, they may grant access also to minors below 13 years by means of accounts that are created and supervised by their guardian

Strengthen the protection of minors through safety-by-design requirements by clarifying the obligations of digital services and certain systems, so that risks to children are addressed in the design and functioning of those services and systems.

Ensure reliable and fundamental rights' compliant age assurance mechanisms by establishing clear requirements and criteria for the use of age assurance systems to support both the access delay and the implementation of safety-by-design measures.

Ensure effective enforcement across the EU by establishing a robust and coherent regulatory and enforcement framework that enables timely and efficient implementation, making sure that minors are protected quickly and effectively in practice.

1.3.3. Expected result(s) and impact

Specify the effects which the proposal/initiative should have on the beneficiaries/groups targeted.

The proposal is expected to contribute to a safer online environment for children while also improving the functioning of the internal market. By clarifying and further harmonising child protection obligations across the Union, it should reduce regulatory fragmentation and provide a more predictable framework for cross-border service and system provision, in particular given the cross-border nature of the providers in scope of this Regulation.

In the short-term, for providers of affected services and systems, the proposal may increase internal compliance costs, require products redesigns and the implementation of additional safety measures – such as age assurance or guardian control tools – and could create certain barriers to entry for some providers. Over time, however, clearer legal obligations are expected to reduce costs, support more level competitive conditions, and facilitate supervision and enforcement by public authorities, with overall impacts expected to be neutral to slightly positive for public authorities.

The proposal is also expected to encourage innovation in child-safe design and age-appropriate digital services and systems, including privacy-preserving age assurance solutions. While costs will increase for age verification or alternative age assurance, synergies with wider Union digital infrastructure, notably the EU Digital Identity Wallet and the EU Age Verification Blueprint, may reduce implementation costs over time.

1.3.4. Indicators of performance

Specify the indicators for monitoring progress and achievements.

The following core indicators have been identified:

Limit access to high-risk digital services and systems: 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 (1). For example, across six countries, 34% of 9–11-year-olds report having a social media profile (2). Against that background, the target would be to

ensure that a substantial proportion of services apply effective access restrictions in line with the new requirements. The recent experience in Australia illustrates that such a societal change takes time and requires not only the effective compliance of providers, but also a shift with minors, parents, and society as a whole. Therefore, success will require effective enforcement, awareness raising in society, broad societal engagement, continuous monitoring and the recognition that behavioural change takes time.

Implement safety-by-design requirements: Currently, the online environment has not been designed with children in mind and does not cater for their evolving capabilities. 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 and, as children are early adopters of new technologies, they also remain the most vulnerable to its risks. Against this background, the target would be to ensure that the online environment becomes safer for minors through the implementation of safety-by-design measures. Success will require that safety of minors is built into products and services from the start, and throughout the lifecycle of a product or service, creating an overall shift-change amongst regulated services and systems that minors' protection should be prioritised. This should be combined with effective enforcement and supervision.

Have in place fundamental rights' compliant age assurance systems. Existing age requirements on online platforms 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 (3). As noted by the OECD, the rationales behind the ages chosen by platforms derive from privacy and contract laws reasons rather than based on an assessment of safety or developmental appropriateness (4). 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 (5). 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 (6, 7, 8). A range of surveys shows that minors routinely mis-state their age online (9). In practice, underage users can therefore easily access many age-restricted online services. In this context, the target is the broad take up of fundamental rights' preserving age assurance. This can be achieved through action and real compliance from the services in scope of the Regulation, combined with effective supervision and enforcement, as well as continuous monitoring and evaluation especially concerning the impacts on fundamental rights.

Strengthen effective enforcement. Enforcement of Regulation (EU) 2022/2065 is running at full speed, including in the area of protection of minors. However, it still takes time before a final non-compliance decision is adopted. Against this background, where non-compliance is suspected, the target is that this is quickly tackled to ensure that minors are quickly served with effective action to protect them in the online environment.

1.4. The proposal/initiative relates to:

X a new action

☐ a new action following a pilot project / preparatory action[10]

X the extension of an existing action

☐ a merger or redirection of one or more actions towards another/a new action

1.5. Grounds for the proposal/initiative

1.5.1. Requirement(s) to be met in the short or long term including a detailed timeline for roll-out of the implementation of the initiative

The protection of minors online requires both immediate action to address urgent risks and structural measures to build a safer digital environment over time.

In the short-term, priority should be given to effective implementation and enforcement of the rules so that minors are effectively protected online – this will require substantial resources to make this a reality in practice. This should be combined with targeted support measures and awareness raising campaigns by Member States for minors, guardian and educators.

In the long-term, the objective is not only to respond to the risks, but to reshape the online environment so that the protection of minors because built-in rather than a corrective measure. This requires sustained investment in privacy-preserving age assurance solutions, strong digital literacy by Member States and the overall development of child-friendly services.

Six months after the entry into application of the Regulation, service providers will have to comply with the social media start date by establishing whether accounts belong to recipients below the minimum age and take measures to disable these. In order to ensure that existing accounts are brought into compliance with the minimum age obligations, providers of very large online platforms shall, before the expiry of the six month time period, submit to the competent authority a detailed implementation plan that corroborates the required high degree of confidence.

As of this date, platforms must also comply with safety-by-design obligations and, where necessary, employ age verification. At the same time, six months after entry into application, the Commission must be ready to enforce the new rules towards Very Large Online Platforms (VLOPs) and Search Engines (VLOSEs), and national Digital Services Coordinators towards smaller platforms and video games. The enforcement for the new requirements for AI companions and chatbots will take place under the existing supervisory and enforcement framework of the AI Act where the Commission is responsible for the AI companions and chatbots built on general-purpose AI models or integrated into VLOPs or VLOSEs.

Twelve months after entry into application, providers of services and systems in scope will have to enable parental accounts, comply with rules for AI companions and general conversational chatbots, implement various flanking measures, as well as follow a code of conduct for age rating if applicable to them. From this date onwards, i.e. twelve months after entry into application of the Regulation, the Commission must be ready to apply the new expedited enforcement regime (30 days for coming to preliminary findings, 90 days for coming to a final decision).

[10] As referred to in Article 58(2), point (a) or (b) of the Financial Regulation.

1.5.2. Added value of EU involvement (it may result from different factors, e.g. coordination gains, legal certainty, greater effectiveness or complementarities). For the purposes of this section 'added value of EU involvement' is the value resulting from EU action, that is additional to the value that would have been otherwise created by Member States alone.

EU action is justified by the cross-border nature of digital services and AI systems, fragmented national approaches regarding restricting minors' access and the need to ensure a consistent level of protection for minors across the Union. Action at EU level can reduce regulatory divergence, increase legal certainty and reducing compliance costs for providers and users, improve enforcement, and ensure that minors are effectively protected throughout the EU.

1.5.3. Lessons learned from similar experiences in the past

Based on Regulation (EU) 2022/2065 there are the following lessons learnt:

Sufficient and stable resources are crucial. Experience under Regulation (EU) 2022/2065 shows that effective enforcement of rules towards the largest companies in the world requires high-skilled resources, technical capacity and sufficient staffing. This is particularly important when supervising and enforcing large cross-border digital services, and doing so in a highly litigious environment.

Resources should be permanent. Enforcement in the digital environment should rely on stable resources, to ensure long-term reliability and predictability. Risks on digital services evolve quickly, and platforms change their systems rapidly, while supervision must be continuous and circumvent the risk of revolving doors. Only through permanent resources can oversight be potent and credible overtime.

Swift enforcement is critical in the online environment, especially for minors. For digital services, harms can scale rapidly and delays can significantly reduce the effectiveness of intervention. Therefore, the enforcement framework must allow for timely action, including the ability to react quickly where serious risks emerge.

Credible enforcement strengthens compliance. Where authorities have the capacity and tools to act decisively, this creates incentives for providers to engage seriously and comply more proactively. Effective supervision is therefore about ensuring that the rules have practical impact.

1.5.4. Compatibility with the multiannual financial framework and possible synergies with other appropriate instruments

The initiative is compatible with the current Multiannual Financial Framework (MFF).

The initiative will draw on a supervisory fee to be paid by each provider of online social networking services, video-sharing platform services, and software application stores for which the Commission enjoys competence to supervise their compliance and that is designated as a very large online platform pursuant to Article 33 of Regulation (EU) 2022/2065, and AI companions, and general conversational chatbots that qualify as a very large online platform. The annual supervisory fee will be calculated based on Art. 43 of Regulation (EU) 2022/2065, which will however not be increased on a given provider of very large online platform or very large search engine for more than 0,03 % of its worldwide annual net income in the preceding financial year.

1.5.5. Assessment of the different available financing options, including scope for redeployment

The preferred financing option is a top up to the existing supervisory fee under the DSA. To this end, providers of online social networking services, of video-sharing platform services, and software application stores which fall under supervision by the European Commission and which are designated as Very Large Online Platform under Regulation (EU) 2022/2065, and AI companions and general conversational chatbots that qualify as a very large online platform will be charged an additional fee to the annual supervisory fee pursuant to Article 43 of Regulation (EU) 2022/2065.

For the purposes of enforcing the rules under this initiative, the Commission will rely partly on redeployment. However, carrying the considerable new supervisory tasks without risking to jeopardise existing enforcement work excludes full reliance on redeployment. See also section 4.1 of the annex.

Where enforcement relies on supervisory fees, it should be pointed out that there will be an inevitable gap between the upfront need for human resources and the financial contribution originating from the supervisory fee which will only become available after the Regulation has entered into force and the fee has been paid. This gap poses a critical risk for the correct implementation of the proposal, as the necessary resources would not be available when they are needed, i.e. from the moment of entry into force. The political and public expectations for effective supervision and enforcement to protect minors online are high, and the Commission will have to demonstrate convincingly that it is able to reign in harmful behaviour. It is therefore of the highest importance to minimise the risk from the gap between the upfront need for human resources and the financial contribution originating from the original fee and ensure that the Commission will have the adequate resources to enforce the proposal from the first day of entry into force.

1.6. Duration of the proposal/initiative and of its financial impact

☐ **limited duration**

– ☐ in effect from [DD/MM]YYYY to [DD/MM]YYYY

– ☐ financial impact from YYYY to YYYY for commitment appropriations and from YYYY to YYYY for payment appropriations.

X unlimited duration

– Implementation with a start-up period from 2028 to unlimited,

– followed by full-scale operation.

1.7. Method(s) of budget implementation planned[11]

X Direct management by the Commission

– **X** by its departments, including by its staff in the Union delegations;

– ☐ by the executive agencies

☐ **Shared management** with the Member States

☐ **Indirect management** by entrusting budget implementation tasks to:

– ☐ third countries or the bodies they have designated

– ☐ international organisations and their agencies (to be specified)

– ☐ the European Investment Bank and the European Investment Fund

– ☐ bodies referred to in Articles 70 and 71 of the Financial Regulation

– ☐ public law bodies

– ☐ bodies governed by private law with a public service mission to the extent that they are provided with adequate financial guarantees

– ☐ bodies governed by the private law of a Member State that are entrusted with the implementation of a public-private partnership and that are provided with adequate financial guarantees

– ☐ bodies or persons entrusted with the implementation of specific actions in the common foreign and security policy pursuant to Title V of the Treaty on European Union, and identified in the relevant basic act

– ☐ bodies established in a Member State, governed by the private law of a Member State or Union law and eligible to be entrusted, in accordance with sector-specific rules, with the implementation of Union funds or budgetary guarantees, to the extent that such bodies are controlled by public law bodies or by bodies governed by private law with a public service mission, and are provided with adequate financial guarantees in the form of joint and several liability by the controlling bodies or equivalent financial guarantees and which may be, for each action, limited to the maximum amount of the Union support.

Comments

None

[11] Details of budget implementation methods and references to the Financial Regulation may be found on the BUDGpedia site: https://myintracomm.ec.europa.eu/corp/budget/financial-rules/budget-implementation/Pages/implementation-methods.aspx.

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

The proposal will be rigorously evaluated, notably in terms of the effectiveness of the access delay, the personal scope of the access delay and its proportionality and the safety by design requirements. This evaluation shall account for experience gained in the implementation of the proposal as well as technological, market and legal developments. The Commission will monitor the application of this Regulation and submit a report to the European Parliament and the Council by 31 August 2030.

Where appropriate, the report will be accompanied by a proposal to amend the Regulation. After this initial review, the Commission will submit a further report to the European Parliament and the Council every four years on progress towards achieving the Regulation's objectives.

This will complement ongoing monitoring under the Digital Services Act.

2.2. Management and control system(s)

2.2.1. Justification of the budget implementation method(s), the funding implementation mechanism(s), the payment modalities and the control strategy proposed

The Regulation establishes a safer online environment for children while also improving the functioning of the internal market. It sets out clear rules to limit minors' access to digital services and systems that present the highest risks to them, strengthen the protection of minors through safety-by-design requirements, establishing clear requirements and criteria for the use of age assurance systems to support both the access delay and the implementation of safety-by-design measures, and putting in place effective enforcement across the EU by establishing a robust and coherent regulatory and enforcement framework

In order for the Commission to carry out the new responsibilities assigned to it, it is necessary to appropriately resource the Commission's services. This is especially important because, in exercising its tasks, the Commission will have to supervise some of the financially strongest and technologically most sophisticated companies in the world, in a highly litigious environment. Supervising these companies will require staff with highly skilled and specialised profiles. The Commission faces a significant political risk if enforcement is under-resourced, especially because this instrument deals with the protection of minors as some of the most vulnerable members of society. Calls for quick action to protect European children online are growing, and making sure that the next generation is effectively protected requires adequate staffing, especially to enable the Commission to deliver on the fast-track enforcement that will be required by the new legislative instrument with a view to protecting children adequately and quickly.

The implementation and enforcement of the Regulation is estimated to require a total of 85 FTE. The proposed staffing levels are proportional to the volume and complexity of the new responsibilities and reflect the most cost-efficient option, avoiding duplication at national level.

In order to ensure these resources are available, the Commission will redeploy 45 FTE. Moreover, in order to complement the resource needs and fulfil the significant new supervisory tasks under this instrument, the Commission will require 40 FTE of new staff.

For financing the supervision of the rules under this instrument, the Commission will rely on a 'top up' to the existing supervisory fee under the Digital Services Act, which will have to be paid by those providers in scope of the new instrument that are designated as VLOP under the Digital Services Act.

Like the Digital Services Act, this legislative proposal meets the three cumulative requirements for relying on a fee:

- A service is being provided: The service concerns the supervision of activities, i.e. the supervision of the compliance of with the Regulation. Supervision has tangible compliance benefits for affected entities. For example, where providers can demonstrate that they are a child-friendly service, they may grant access also to minors below 13 years by means of accounts that are created and supervised by their guardian. The costs related to the provision of the service include the costs of IT tools, staff costs, and other administrative costs.

- The service is individually received by those who pay the contribution: The service provides direct benefits for the entities who are requested to pay the fee. By undergoing the supervision services provided for in the proposal, providers can reliably prove that they are offering a service that is safe for minors. The top-up to the DSA supervisory fee under this instrument will only be paid by those entities that are in scope of the new instrument and, by virtue of their designation as VLOPs or VLOSE under the DSA, fall under the Commission's direct supervision.

- Proportionate fee level: As per established practice under the Digital Services Act, the level of the fee (and its top-up) will be established annually and will, in volume, be tailored to the individual supervised entity by use of a formula that takes into account the service's number of users and may and is capped at a level of the service provider's worldwide profit in the preceding financial year. The maximum top-up for the supervisory activities under this new instrument on a given provider of very large online platform or very large search engine is capped at 0,03 % of its worldwide annual net income in the preceding financial year.

As with the Digital Services Act, this instrument constitutes a case where the permanent nature of the revenue and the permanent nature of the tasks performed in exchange for the fee can be ensured. The DSA supervisory fee has been collected since 2024. So far, it amounted to between EUR 40 and 60 million annually, with slight variations explained by changes in the expected supervision costs for the following year. The pool of VLOPSEs (> 45 million monthly active users), has continued to grow rather than shrink as more services cross the user-number threshold. The underlying revenue base of the new fee can thus be considered stable, as services with > 45 million monthly active users are unlikely to rapidly lose user numbers and be removed from Commission supervision.

The permanent nature of the DSA fee, coupled with the permanence and significance of the Commission's supervisory tasks regarding the safety and trustworthiness of online platforms including for safeguarding children online, renders the DSA and the

current instrument a suitable example of an area in which the underlying fee could finance establishment plan posts.

2.2.2. Information concerning the risks identified and the internal control system(s) set up to mitigate them

The activities proposed in the Regulation involve the Commission and national authorities to carry out supervisory activities. The Commission will have to ensure that such activities are sufficiently staffed, and also that it is ready to prepare delegated and implementing acts, guidance documents, comitology secretariat, including monitoring against established KPIs and milestones. This would allow to promptly identify possible issues and risks in the execution of its activities.

Furthermore, for the revenues stemming from the supervisory fee, the Regulation will provide for regular reporting obligations for the Commission as regards the costs incurred and the revenues collected.

However, it should be pointed out that there will be an inevitable gap between the upfront need for human resources and the financial contribution originating from the supervisory fee which will only become available after the Regulation has entered into force and the fee paid.

This gap poses a critical risk for the correct implementation of this Regulation, as the necessary resources would not be available when they are needed, i.e. from the moment of entry into force. The political and public expectations for effective supervision and enforcement to achieve the objectives of this Regulation are high, and the Commission will have to demonstrate convincingly that it is able to reign in behaviour and impose changes where warranted.

It is therefore of the highest importance to minimise the risk from the gap between the upfront need for human resources and the financial contribution originating from the original fee and ensure that the Commission will have the adequate resources to enforce the new initiative from the first day of entry into force. Redeploying existing staff for parts of the supervisory activities under this new initiative is a key mitigation strategy in this regard.

2.2.3. Estimation and justification of the cost-effectiveness of the controls (ratio between the control costs and the value of the related funds managed), and assessment of the expected levels of risk of error (at payment & at closure)

The cost of controls for this initiative have been estimated at Commission level. The source of this information is the Commission's internal management and control system. The costs were estimated based on the staff and resources dedicated to the activities foreseen as part of this initiative. The expected total costs for such controls can be relatively high due to the complexity of the activities proposed and the need for dedicated resources to mitigate execution risks. The control intensity will be adapted to the nature of the expenditure, the type of beneficiaries or contractors foreseen, the amount of financial resources concerned, and the level of risk.

2.3. Measures to prevent fraud and irregularities

The existing fraud prevention measures applicable to the Commission will cover the additional appropriations necessary for this Regulation. In addition, this Regulation will provide for regular reporting on the costs incurred and revenues collected from

the supervisory fee and mechanisms to adjust the level of the fees to the costs incurred.

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

The estimated impact on expenditure and staffing for 2028 and beyond is added for illustrative purposes only and does not pre-judge the next Multiannual Financial Framework. The source of financing and scope of Union financial commitment in the post-2027 period remain subject to the outcome of interinstitutional negotiations on the MFF 2028-2034 and thereafter shall be determined through the annual budgetary procedure. All appropriations and staffing allocations as of 2028 are indicative.

3.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected

- Existing budget lines

In order of multiannual financial framework headings and budget lines.

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Number	Diff./Non-diff.[12]	from EFTA countries [13]	from candidate countries and potential candidates [14]	From other third countries	other assigned revenue
	02 20 03 05 Digital Services Act (DSA) – Supervision of very large online platforms	Diff.	NO	NO	NO	YES

- New budget lines requested

In order of multiannual financial framework headings and budget lines.

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Number	Diff./Non-diff.	from EFTA countries	from candidate countries and potential candidates	from other third countries	other assigned revenue

12 Diff. = Differentiated appropriations / Non-diff. = Non-differentiated appropriations.

13 EFTA: European Free Trade Association.

14 Candidate countries and, where applicable, potential candidates from the Western Balkans.

3.2. Estimated financial impact of the proposal on appropriations

3.2.1. Summary of estimated impact on operational appropriations

– ☐ The proposal/initiative does not require the use of operational appropriations

– ☒ The proposal/initiative requires the use of operational appropriations, as explained below

3.2.1.1. Appropriations from voted budget

3.2.1.2. Appropriations from external assigned revenues

EUR million (to three decimal places)

Heading of multiannual financial framework	Number	

DG CONNECT			Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**	Year **2033**	Year **2034**	**TOTAL MFF 2028-2034**
Operational appropriations										
DSA fee	Commitments	(1a)	7.700	5.700	5.700	5.700	5.700	5.700	5.700	**41.900**
	Payments	(2a)	5.700	5.700	7.700	5.700	5.700	5.700	5.700	**41.900**
Budget line	Commitments	(1b)								**0**
	Payments	(2b)								**0**
Appropriations of an administrative nature financed from the envelope of specific programmes[15]										
Budget line		(3)								**0**
TOTAL appropriations	Commitments	=1a+1b+3	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**

[15] Technical and/or administrative assistance and expenditure in support of the implementation of EU programmes and/or actions (former 'BA' lines), indirect research, direct research.

for DG CONNECT	Payments		=2a+2b+3	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**			

			Year	Year	Year	Year	Year	Year	Year	**TOTAL MFF 2028-2034**
			2028	**2029**	**2030**	**2031**	**2032**	**2033**	**2034**	
TOTAL operational appropriations	Commitments	(4)	7.700	5.700	5.700	5.700	5.700	5.700	5.700	**41.900**
	Payments	(5)	5.700	5.700	7.700	5.700	5.700	5.700	5.700	**41.900**
TOTAL appropriations of an administrative nature financed from the envelope for specific programmes		(6)	0	0	0	0	0	0	0	**0**
TOTAL appropriations under HEADING <….> of the multiannual financial framework	Commitments	=4+6	7.700	5.700	5.700	5.700	5.700	5.700	5.700	**41.900**
	Payments	=5+6	5.700	5.700	7.700	5.700	5.700	5.700	5.700	**41.900**

Heading of multiannual financial framework	4	‘Administrative expenditure’[16]

EUR million (to three decimal places)

DG CONNECT		Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**	Year **2033**	Year **2034**	**TOTAL MFF 2028-2034**
• Human resources		2.020	2.020	2.020	2.020	2.020	2.020	2.020	**14.140**
• Other administrative expenditure		0	0	0	0	0	0	0	**0**
TOTAL DG CONNECT	Appropriations	2.020	2.020	2.020	2.020	2.020	2.020	2.020	**14.140**

16 The necessary appropriations should be determined using the annual average cost figures available on the appropriate BUDGpedia webpage.

TOTAL appropriations under HEADING 4 of the multiannual financial framework	(Total commitments = Total payments)	**2.020**	**2.020**	**2.020**	**2.020**	**2.020**	**2.020**	**2.020**	**14.140**

EUR million (to three decimal places)

		Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**	Year **2033**	Year **2034**	**TOTAL MFF 2028-2034**
TOTAL appropriations under HEADINGS 1 to 4	Commitments	**9.720**	**7.720**	**7.720**	**7.720**	**7.720**	**7.720**	**7.720**	**56.040**
of the multiannual financial framework	Payments	**7.720**	**7.720**	**9.720**	**7.720**	**7.720**	**7.720**	**7.720**	**56.040**

3.2.2. Estimated output funded from operational appropriations (not to be completed for decentralised agencies)

Commitment appropriations in EUR million (to three decimal places)

Indicate objectives and outputs ⇩			Year **2028**		Year **2029**		Year **2030**		Year **2031**		Enter as many years as necessary to show the duration of the impact (see Section1.6)						**TOTAL**	
	OUTPUTS																	
	Type[17]	Average cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	Total No	Total cost
SPECIFIC OBJECTIVE No 1[18]…																		
- Output																		
- Output																		

17 Outputs are products and services to be supplied (e.g. number of student exchanges financed, number of km of roads built, etc.).

18 As described in Section 1.3.2. 'Specific objective(s)'

- Output																		
Subtotal for specific objective No 1																		
SPECIFIC OBJECTIVE No 2 ...																		
- Output																		
Subtotal for specific objective No 2																		
TOTALS																		

3.2.3. Summary of estimated impact on administrative appropriations

– ☐ The proposal/initiative does not require the use of appropriations of an administrative nature

– ✠ The proposal/initiative requires the use of appropriations of an administrative nature, as explained below

3.2.3.1. Appropriations from voted budget

VOTED APPROPRIATIONS	Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**	Year **2033**	Year **2034**	**TOTAL 2028 - 2034**
HEADING 4								
Human resources	2.020	2.020	2.020	2.020	2.020	2.020	2.020	**14.140**
Other administrative expenditure	0.000	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**
Subtotal HEADING 4	**2.020**	**2.020**	**2.020**	**2.020**	**2.020**	**2.020**	**2.020**	**14.140**
Outside HEADING 4								
Human resources	0.525	0.525	0.525	0.525	0.525	0.525	0.525	**3.675**
Other expenditure of an administrative nature	0.000	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**
Subtotal outside HEADING 4	**0.525**	**0.525**	**0.525**	**0.525**	**0.525**	**0.525**	**0.525**	**3.675**
TOTAL	**2.545**	**2.545**	**2.545**	**2.545**	**2.545**	**2.545**	**2.545**	**17.815**

3.2.3.2. Appropriations from external assigned revenues

EXTERNAL ASSIGNED REVENUES	Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**	Year **2033**	Year **2034**	**TOTAL 2028 - 2034**
HEADING 4								
Human resources	0.000	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**
Other administrative expenditure	0.000	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**
Subtotal HEADING 4	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**
Outside HEADING 4								
Human resources	10.175	10.175	10.175	10.175	10.175	10.175	10.175	**71.228**
Other expenditure of an administrative nature	0.000	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**
Subtotal outside HEADING 4	**10.175**	**10.175**	**10.175**	**10.175**	**10.175**	**10.175**	**10.175**	**71.228**
TOTAL	**10.175**	**10.175**	**10.175**	**10.175**	**10.175**	**10.175**	**10.175**	**71.228**

3.2.3.3. Total appropriations

TOTAL VOTED APPROPRIATIONS + EXTERNAL ASSIGNED REVENUES	Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**	Year **2033**	Year **2034**	**TOTAL 2028 - 2034**

			HEADING 4					
Human resources	2.020	2.020	2.020	2.020	2.020	2.020	2.020	**14.140**
Other administrative expenditure	0.000	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**
Subtotal HEADING 4	**2.020**	**2.020**	**2.020**	**2.020**	**2.020**	**2.020**	**2.020**	**14.140**
				Outside HEADING 4				
Human resources	10.700	10.700	10.700	10.700	10.700	10.700	10.700	**74.903**
Other expenditure of an administrative nature	0.000	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**
Subtotal outside HEADING 4	**10.700**	**10.700**	**10.700**	**10.700**	**10.700**	**10.700**	**10.700**	**77.903**
TOTAL	**12.720**	**12.720**	**12.720**	**12.720**	**12.720**	**12.720**	**12.720**	**89.043**

The appropriations required for human resources and other expenditure of an administrative nature will be met in part by appropriations from the DG that are already assigned to management of the action and/or have been redeployed within the DG, together with any additional resources that will be paid by the DSA fee as external assigned revenue and limited recourse to the administrative budget.

3.2.4. Estimated requirements of human resources

– ☐ The proposal/initiative does not require the use of human resources

– ☒ The proposal/initiative requires the use of human resources, as explained below

3.2.4.1. Financed from voted budget

Estimate to be expressed in full-time equivalent units (FTEs)[19]

VOTED APPROPRIATIONS		Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**	Year **2033**	Year **2034**
• Establishment plan posts (officials and temporary staff)								
20 01 02 01 (Headquarters and Commission's Representation Offices)		5	5	5	5	5	5	5
20 01 02 03 (EU Delegations)		0	0	0	0	0	0	0
(Indirect research)		0	0	0	0	0	0	0
(Direct research)		0	0	0	0	0	0	0
Other budget lines (specify)		0	0	0	0	0	0	0
• External staff (in FTEs)								
20 02 01 (AC, END from the 'global envelope')		10	10	10	10	10	10	10
20 02 03 (AC, AL, END and JPD in the EU Delegations)		0	0	0	0	0	0	0
Admin. Support line	• at Headquarters	0	0	0	0	0	0	0
[XX.01.YY.YY]	• in EU Delegations	0	0	0	0	0	0	0
(AC, END - Indirect research)		0	0	0	0	0	0	0

[19] Please specify below the table how many FTEs within the number indicated are already assigned to the management of the action and/or can be redeployed within your DG and what are your net needs.

(AC, END - Direct research)	0	0	0	0	0	0	0
Other budget lines (specify) - Heading 4	0	0	0	0	0	0	0
Other budget lines (AI Office) - Outside Heading 4	5	5	5	5	5	5	5
TOTAL	**20**	**20**	**20**	**20**	**20**	**20**	**20**

3.2.4.2. Financed from external assigned revenues

EXTERNAL ASSIGNED REVENUES	Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**	Year **2033**	Year **2034**
• Establishment plan posts (officials and temporary staff)							
20 01 02 01 (Headquarters and Commission's Representation Offices)	0	0	0	0	0	0	0
20 01 02 03 (EU Delegations)	0	0	0	0	0	0	0
(Indirect research)	0	0	0	0	0	0	0
(Direct research)	0	0	0	0	0	0	0
Other budget lines (DSA fee)	15	15	15	15	15	15	15
• External staff (in full time equivalent units)							
20 02 01 (AC, END from the 'global envelope')	0	0	0	0	0	0	0
20 02 03 (AC, AL, END and JPD in the EU Delegations)	0	0	0	0	0	0	0
Admin. Support line [XX.01.YY.YY] • at Headquarters	0	0	0	0	0	0	0
Admin. Support line [XX.01.YY.YY] • in EU Delegations	0	0	0	0	0	0	0
(AC, END - Indirect research)	0	0	0	0	0	0	0
(AC, END - Direct research)	0	0	0	0	0	0	0
Other budget lines (specify) - Heading 4	0	0	0	0	0	0	0
Other budget lines (DSA fee) - Outside Heading 4	50	50	50	50	50	50	50
TOTAL	**65**	**65**	**65**	**65**	**65**	**65**	**65**

3.2.4.3. Total requirements of human resources

TOTAL VOTED APPROPRIATIONS + EXTERNAL ASSIGNED REVENUES	Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**	Year **2033**	Year **2034**
• Establishment plan posts (officials and temporary staff)							
20 01 02 01 (Headquarters and Commission's Representation Offices)	5	5	5	5	5	5	5
20 01 02 03 (EU Delegations)	0	0	0	0	0	0	0
(Indirect research)	0	0	0	0	0	0	0
(Direct research)	0	0	0	0	0	0	0

Other budget lines (DSA fee)		15	15	15	15	15	15	15
• External staff (in full time equivalent units)								
20 02 01 (AC, END from the 'global envelope')		10	10	10	10	10	10	10
20 02 03 (AC, AL, END and JPD in the EU Delegations)		0	0	0	0	0	0	0
Admin. Support line [XX.01.YY.YY]	• at Headquarters	0	0	0	0	0	0	0
	• in EU Delegations	0	0	0	0	0	0	0
(AC, END - Indirect research)		0	0	0	0	0	0	0
(AC, END - Direct research)		0	0	0	0	0	0	0
Other budget lines (specify) - Heading 4		0	0	0	0	0	0	0
Other budget lines (ECF Digital window – administrative support line and DSA fee) - Outside Heading 4		55	55	55	55	55	55	55
TOTAL		**85**	**85**	**85**	**85**	**85**	**85**	**85**

Possible internal redeployment within the Commission are for duly substantiated reasons insufficient. The proposal therefore requires additional human resources in DG CONNECT. The financing of these additional resources will be mainly the DSA fee as external assigned revenue, with limited recourse to the administrative budget.

The staff required to implement the proposal (in FTEs):

	Internally redeployed		**Exceptional additional staff**		
	Within the implementing DGs*	**Exceptionally, from the Commission redeployment pool after orientation from the CMB****	**To be financed from Heading 7*** / Research**	**To be financed from BA line**	**To be financed from fees**
Establishment plan posts	5				15
External staff (CA, SNEs, INT)	35 (already financed under the DSA fee) 5 (AI Office)	10			15
Total	45	10			30

The scale, significance and required speed of new supervisory tasks entrusted to the European Commission exceeds what can be covered by existing human resources and internal redeployments within the Commission.

Compared to the existing enforcement frameworks under the Digital Services Act and the AI Act, this instrument places a number of new supervisory tasks in the hands of the Commission – chief among

them the enforcement of the delayed access of minors to social networking services and video-sharing platform services but also important elements such as the supervision of safety-by-design requirements to be implemented by providers of online social network services, of video-sharing platform services as well as of AI companions and general conversational chatbots, where these falls under Commission supervision.

The enforcement of these new rules is of exceptionally high social significance as they are designed to safeguard some of the most vulnerable members of society: Children. The underlying evidence shows the significant developmental and health risks to which children are exposed online. These risks necessitate the new rules and make their enforcement a task of utmost societal significance. The political and public expectations, including from Member States, for effective supervision and enforcement to protect minors online are high, and the Commission will have to demonstrate convincingly that it is able to reign in harmful behaviour.

Because of the heightened risk that children face online, this instrument foresees a fast-track enforcement path, which requires the Commission to adopt preliminary findings within 30 working days and a final decision within 90 working days. These enforcement timelines are unprecedented. The Commission will be required to enforce the new rules of this instrument not just in an expedited fashion, but also towards the largest and most well-resourced companies in the world in a highly litigious environment.

Taken together, these factors render it impossible to rely purely on existing human resources and internal redeployments.

The requested additional staff would lead to increase the authorised staffing levels under the DSA by 30 FTEs (15 permanent and 15 non-permanent), financed from the DSA fee (external assigned revenue). Additionally, 10 FTE of non-permanent staff would be redeployed within the Commission to reinforce the staffing levels of the AI Office.

Description of tasks to be carried out by:

Officials and temporary staff	• Day-to-day monitoring, supervision and oversight for VLOPSEs or AI companions and chatbots under the Commission supervision dealing in particular with: • Monitoring of providers' behaviour, including regular and continuous analysis, including review of the reports on the effectiveness of the measures, regular review of transparency documents produced through the DSA or the new instrument, e.g. transparency reports, risk assessments, data access requests, etc., and requests for access to data/algorithms, test and support to the analysis • Continuous work on age assurance including continued work on the EU Age Verification Blueprint and on the EU Age Verification Scheme, assessment of alternative age verification and age assurance solutions, work on technical standards, work with Member States on identity and credential architectures, and develop the governance of trusted issuers and relying parties. • Implementation of the EU Age Verification System, including the compliance assessment of candidate providers of EU age verification solutions and candidate providers of EU proof of age attestations and the management of the infrastructure related to it. • Coordination/cooperation with Digital Services Coordinators (DSCs)/ Market Surveillance Authorities (MSAs), the Digital Services or AI Board and SICs • Operation of a 24/7 crisis capability • Research and foresight to keep abreast of fast-changing developments and be aware of changing impacts on society, e.g. related to minors and health

	• Enforcement proceedings and supervision of remedies: • Expedited procedures to take quick action in case of non-compliance, including taking investigatory steps such as requests for information, interviews, analysis of algorithms, inspections, analysis of commitments, assessment of action plans • Coordination with DSCs/MSAs on investigatory steps, e.g. working with DSCs/MSAs on investigations, assessing DSCs/MSAs reasoned requests for action, consultation/information sharing within the Board • Support of the general cross-border cooperation and enforcement, including: • Assessment of DSCs/MSAs measures on services/systems within their responsibilities • Support to the Board, including preparation of agenda of the meetings, organization of working groups and draft documents • Other regulatory measures • Adoption of delegated and implementing acts as well as guidance documents (including additional acts/guidance requested by EP Report); • Codes of conduct and standardisation • Flanking measures • Support Member States as they promote and take measures for the development of digital literacy skills and in the development of assistance channels, in accordance with Article 32 of the new legislative instrument • Facilitate exchange of best practices, including on the development of digital literacy skills, national support channels and applications – and issue guidelines. • International outreach and interaction with third country regulators/enforcement authorities.
External staff	• Contribute to the handling of implementation and enforcement activities • Support document-related tasks in support of case teams, including by ensuring due filing and consistency with the procedural principles and timelines • Prepare correspondence with the supervised entities and prepare access to the case files • Background research and analysis

3.2.5. Overview of estimated impact on digital technology-related investments

Compulsory: the best estimate of the digital technology-related investments entailed by the proposal/initiative should be included in the table below.

Exceptionally, when required for the implementation of the proposal/initiative, the appropriations under Heading 4 should be presented in the designated line.

The appropriations under Headings 1-3 should be reflected as "Policy IT expenditure on operational programmes". This expenditure refers to the operational budget to be used to re-use/ buy/ develop IT platforms/ tools directly linked to the implementation of the initiative and their associated investments (e.g. licences, studies, data storage etc). The information provided in this table should be consistent with details presented under Section 4 "Digital dimensions".

TOTAL Digital and IT appropriations	Year 2028	Year 2029	Year 2030	Year 2031	Year 2032	Year 2033	Year 2034	TOTAL MFF 2028 - 2034
HEADING 4								
IT expenditure (corporate)	0	0	0	0	0	0	0	**0**
Subtotal HEADING 4	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
Outside HEADING 4								
Policy IT expenditure on operational programmes	0	0	0	0	0	0	0	**0**
Subtotal outside HEADING 4	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
TOTAL	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**

3.2.6. Compatibility with the current multiannual financial framework

The proposal/initiative:

– ☐ can be fully financed through redeployment within the relevant heading of the multiannual financial framework (MFF)

– ☐ requires use of the unallocated margin under the relevant heading of the MFF and/or use of the special instruments as defined in the MFF Regulation

– ☐ requires a revision of the MFF

3.2.7. Third-party contributions

The proposal/initiative:

– ☒ does not provide for co-financing by third parties

– ☐ provides for the co-financing by third parties estimated below:

Appropriations in EUR million (to three decimal places)

	Year 2028	Year 2029	Year 2030	Year 2031	Year 2032	Year 2033	Year 2034	Total
Specify the co-financing body								
TOTAL appropriations co-financed								

3.3. Estimated impact on revenue

– ☐ The proposal/initiative has no financial impact on revenue.

– ☒ The proposal/initiative has the following financial impact:

  – ☐ on own resources

  – ☒ on other revenue (assigned)

  – ☐ please indicate, if the revenue is assigned to expenditure lines

EUR million (to three decimal places)

Budget revenue line:	Appropriations available for the current financial year	Impact of the proposal/initiative[20]						
		Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**	Year **2033**	Year **2034**
02 20 03 05		17.875	15.875	15.875	15.875	15.875	15.875	15.875

For assigned revenue, specify the budget expenditure line(s) affected.

02 20 03 05 Digital Services Act (DSA) – Supervision of very large online platforms
Other remarks (e.g. method/formula used for calculating the impact on revenue or any other information).

4. DIGITAL DIMENSIONS

To comply with this Regulation, providers of digital services and systems in scope must determine the age of recipients of the service or the user of the system in compliance with the requirements established in Chapter V. Notably, the implementation of the 'access delay' requires providers of social networking services and video-sharing platforms to put in place robust and effective EU age verification solutions, which are based on the EU age verification blueprint, made available by the Commission. Member States and/or private entities can take this up as a self-standing app or as part of a digital wallet. This solution is user-friendly, secure and fully privacy preserving. For the purposes of implementing safety-by-design obligations, age assurance solutions, other than EU age verification, may also be used to comply with the Regulation, provided that they live up to certain criteria. In order to make this work in practice, it is important that there are age verification and age assurance solutions in place that provide a high level of accuracy, reliability, security, robustness, non-intrusiveness, privacy and data protection and non-discrimination. Commercial solutions are already on the market to determine the age of a recipient of the service, and provided that they provide an sufficient level of protection they may be used in accordance with the provisions of this Regulation.

Furthermore, following the Commission Recommendation (EU) 2026/1035, the Commission is developing an EU Age Verification Scheme, which consists of the requirements concerning the trust model, governance and the requirements to be fulfilled by providers of the proof of age attestation and age verification solutions.

[20] In the case of traditional own resources (customs duties, sugar levies), the amounts indicated must be net amounts, i.e. gross amounts after deduction of 10 % for collection costs, as proposed in COM(2025)574.

Entities should meet the requirements of the EU Age Verification Scheme before their solutions and proof of age attestation providers respectively can be added to EU trusted solutions list. Similarly, the proof of age attestation providers should meet the requirements of the EU Age Verification Scheme before they are added on the EU trusted proof of age attestation providers list. The EU Age Verification Scheme will need its maintenance and operations to be supported in the medium and long term.

4.1. Requirements of digital relevance

It is against this background that the following requirements are established in the Regulation:

Requirement 1 (R1): providers of services subject to access delay are required to propose to recipients of their services and users of the systems to prove their age with EU age verification solutions using an EU proof of age attestation or other solutions as referred to in paragraph 2(a) and 2(b) of Article 24 of the present Regulation.

Requirement 2 (R2): providers subject to the safety-by-design obligations and providers of software application stores may use age assurance solutions other than EU age verification solutions provided that they provide a high level of accuracy, reliability, security, robustness, non-intrusiveness, privacy and data protection, and non-discrimination.

Requirement 3 (R3): the European Commission shall adopt implementing acts covering the existing specifications and the operation of the EU Age Verification Scheme, and a list of issuers of EU proof of age attestations and a list of EU age verification solutions.

As mentioned above, for the purposes of R1 and R2, the Commission has already established the EU Age Verification Blueprint, which now requires uptake by Member States or private companies. For the purposes of R3, the Commission is already establishing the EU Age Verification Scheme as well as the two lists.

For the purposes of information sharing between responsible authorities, AGORA will be used which is a secure information sharing system to support communications between the Digital Services Coordinators (DSCs) in the Member States, the Commission and the European Board for Digital Services (composed of the DSC). The Commission, the DSCs and the Board use AGORA for all communications related to enforcement of the DSA. This system is already established and will now also be used for the purposes of this Regulation, which would potentially require further onboarding of authorities onto the system, although such additional onboarding is likely limited since relevant authorities are mostly already onboarded. Therefore, this will not further be touched upon in this Legislative Financial and Digital Statement. The same applies regarding the supervision and enforcement of the AI companions and chatbots which will rely on the structures, enforcement framework and information exchange system that is already set up under the AI Act.

4.2. Data

The EU age verification solution is a privacy-preserving, data-minimising, non-traceable, unlinkable and double-blind solution designed to keep to an absolute necessary minimum the processing of personal data. In many cases a person’s age can be verified based on existing data available to the issuer of the proof of age attestation. Producing the proof of age attestations involves processing personal data of persons who need to prove their age to online services. This data processing is done separately from the person’s access to such online services. The online service itself receives no personal information about the user as a result of the age verification process, except the proof that the person is over the required

age. This data processing is fully privacy-preserving and uses the latest technology to ensure full compliance with data protection standards. The technology is regularly updated to maintain its secure and privacy-preserving nature. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en

4.3. Digital solutions

The EU Age Verification Scheme is a set of open-source technical requirements that can be used to publish a stand-alone mobile age verification application. It is available to both Member States and private actors to develop an age verification solution.

The solution allows individuals to prove to digital services and systems requiring age verification that they are old enough without sharing their identity, exact age, date of birth, or other personal information. This digital solution supports the digital requirements R1 and R2 and is indirectly linked to R3, by outputting proofs of age attestations, proving that individuals are (or are not) above a certain age.

4.4. Interoperability assessment

The European Age verification solution is technically interoperable with the European Digital Identity Wallets as specified in Regulation (EU) 910//2014 setting out the European Digital Identity Framework. The proof of age attestation will be issued as an electronic attestation of attributes as set out in Article 3 (44) of Regulation (EU) 910/2014. This ensures that age verification solutions and their proof of age attestation providers will provide the (potential) recipients of the service with proof of age attestations that can be used across digital services and across Member States.

The core specificities of the age verification solutions therefore allow for a seamless interoperability across digital services for potential recipients of digital services to prove their age.

4.5. Measures to support digital implementation

As mentioned in Section 4.1 the Commission is already well-underway to support the digital implementation of this Regulation, through the publication of the EU blueprint and the ongoing work on the EU Age Verification Scheme. This should allow that the infrastructure and system is in place at the time of entry into application.

To ensure public uptake, but to also allow for constant public feedback and updating, the European Commission published the technical requirements needed to build EU Age Verification solutions. The project is open source and all the information is available publicly at the website *ageverification.dev*. This website and its associated IT test infrastructure will need ongoing maintenance and operations. Furthermore, the ongoing work on the EU Age Verification Scheme, should make the work on the implementing acts to underpin this work straightforward, as it will be based on existing practice. Awareness raising campaigns around the time of entry into force will be crucial, not only to support wide public uptake, but also to mitigate concerns related to privacy and usability.