



EUROPEAN
COMMISSION

Strasbourg, **XXX**
COM(2026) 680/2

SENSITIVE*
UNTIL ADOPTION

**COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN
PARLIAMENT AND THE COUNCIL**

An EU approach to online child safety

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

EN
EN

EURACTIV

EN
EN

1. Introduction

The digital world is a gateway to knowledge, an opportunity for connection and creativity. But platforms' business models, designed to maximise the time spent online, result in a massive scale of online engagement and may exploit the vulnerabilities of children. According to a 2026 Eurobarometer, teenagers spend on average 4.5 hours online on school days, rising to 6.1 hours on weekend days¹.

The available evidence shows that the earlier children go online, the more time they are likely to spend on screens. Those who started using social media before the age of 10 report 7.5 hours of weekend day screen time, compared to 5.7 hours among those who started after age 14. **This amplifies pressure on youth mental health, which has never been more at risk.** One in three teenagers feel stressed or socially excluded and affected by concentration problems. As confirmed by the results of the OECD's Programme for International Student Assessment (PISA) for 2025, digital distraction impacts young people's learning and is a key factor for declining basic skills in the EU. In addition, one in four children currently encounters harmful and distressing content online, ranging from violence, hate speech, body pressure, and misinformation. One in four also experience online sexual solicitation at some point before age 18, including unwanted/pressured sexual interactions and forms of grooming². While any child may be affected, vulnerable children are disproportionately at risk and girls and boys experience different kinds of risks.

The development of problematic AI-generated content, such as deepfakes or dangerous advice given by AI chatbots, is further exacerbating the issue. Pressure to share intimate pictures affects one in ten teenagers, representing millions of young people across Europe. This is not merely passive exposure and does not remain confined to the screen. Such content shapes, encourages and rewards risky behaviour, from harming others to self-harm, including eating disorders to reckless behaviour performed and filmed to seek attention and validation, with in some cases fatal consequences.

The Union already has strong foundations to protect minors online. The Digital Services Act (DSA) requires online platforms to keep minors safe when considering the core design choices of their services. The EU regulatory framework includes also comprehensive safeguards for children online when using streaming services, online games, online retailers, and AI products. The General Data Protection Regulation (GDPR) provides specific rules and safeguards regarding the use of personal data, including children's. EU consumer protection law, including the Unfair Commercial Practices Directive (UCPD), protects minors as vulnerable consumers.

Enforcing this legislation has been a key Commission priority. Under the DSA, for instance, the Commission took enforcement action against ByteDance and Meta over addictive design of their flagship online platforms TikTok, Facebook and Instagram, respectively, and over inadequate age assurance on Facebook and Instagram. The Commission has also taken enforcement action against X over Grok's generation and dissemination of child sexual abuse material. Through the Consumer Protection Cooperation (CPC) Network, the Commission and national authorities have been addressing harmful

¹ Impact of excessive screen time and social media on young people's mental health - June 2026 - Eurobarometer survey

² <https://www.childlight.org/reports/itl-interim-update-2026>

practices including in online games and e-commerce³. Data Protection Authorities have also taken action against Meta, Tik Tok, X and others regarding the misuse of children's personal data.

However **existing rules do not suffice**. The current EU legislative framework does not specify a minimum age for access to platforms and services with age inappropriate or risky features and content. There is also no outright ban on common problematic features, such as endless scrolling, excess notifications, or harmful recommender systems. Moreover, the existing Union framework does not provide sufficiently strong harmonisation and detail on addressing addictive design features for digital products and services accessible to minors. It also lacks legal certainty regarding age verification systems and legal responsibility of tech companies for the design of their services.

Following the announcement in the 2025 State of the Union address, a **Special Panel** was tasked with advising the Commission President on the development of a European approach to keep children safe online. The Special Panel involved the various stakeholder groups and heard experts from different background, both from the Union and from partner countries. Its deliberations resulted in the report of the Co-Chairs of the Special Panel, setting out their findings and key recommendations⁴.

Alongside, child safety online has been acknowledged as a global challenge requiring close cooperation among partners. In the United States, the recent Meta settlement shows that service providers now realise that they are increasingly regarded, both legally and societally, as responsible for the safety of children to whom they provide services⁵. Within the EU, many Member States are considering different national legislative initiatives to protect minors online, notably by setting out a minimum age to access certain services⁶. **Recent developments have however clearly demonstrated the legal complexity surrounding the issue**, alongside the need for a targeted and proportionate approach and for protecting fundamental rights⁷.

Against this background, **decisive, comprehensive and urgent action at Union level is the most appropriate way forward** to tackle more effectively and swiftly the scale and gravity of the risks encountered by children online. It represents the effective response to unequivocal calls from the European Council, co-legislators and key stakeholders advocating for the need of a common European approach to protect all children equally throughout the Union, as they navigate online. It will support the effectiveness of the EU's external cooperation and the Union's influence with trusted partners and allies.

³ In *Star Stable Online*, for example, the CPC Network investigated direct purchase exhortations towards children, pressure selling tactics and unclear information on in-game currencies, asking the company to put forward commitments to improve its practices. Moreover, CPC coordinated actions are ongoing against Temu and Shein for breaches of consumer law relating to dark patterns, fake discounts, and other unfair commercial practices.

⁴ Child safety online protecting and empowering minors in a digital world, available at https://commission.europa.eu/document/download/d833504d-5ec3-4fac-945f-38e7d0bd5326_en?filename=Special-panel-report.pdf

⁵ <https://www.oag.state.va.us/media-center/news-releases/3105-attorney-general-jay-jones-announces-a-17-billion-landmark-settlement-with-meta-with-353-million-guaranteed-for-virginia>

⁶ Draft legislation is being prepared or negotiated in 17 Member States.

⁷ <https://www.conseil-constitutionnel.fr/decision/2026/2026911DC.htm>

2. Towards a comprehensive and ambitious European approach: the EU KIDS Act

The **Union's approach** should allow minors to benefit from the huge potential of digital services, while protecting them from abuse and exploitation. It **needs to limit the access of tech companies to our children, and not the other way around**. It must stress that the key responsibility to design safe online spaces rest with the digital service providers. It must respect the evolving maturity of children as they grow up, and the role of their guardians, without unduly shifting responsibility to them. The Union's approach should therefore be comprehensive, collective, age-appropriate and based on the actual risks children face online. It should be grounded on children's rights as fundamental rights, in line with the Charter of fundamental rights of the EU, taking the best interests of the child as a primary consideration.

The EU KIDS Act adopted with this Communication **puts forward a single, EU-wide set of rules providing equal level of protection for all children** throughout the Union, alongside a **set of tools for parents and guardians**⁸. The proposal will reduce the risk of fragmentation across Member States and provide clear legal certainty to EU businesses as they navigate the Single Market.

The proposal will apply to "Social Media+" – the group of services that pose the greatest risk to minors. These are the social media services, video-sharing platforms and online games which pose specific design risks for minors, as well as AI Chatbots and AI Companions – as virtual tools that can give mental health and personal development advice to minors. It will not target services that are designed and operated for education or by public authorities, nor will it apply to industrial AI or AI office products. The proposal will comprise a **combined approach** of (i) an **EU-wide minimum age** and (ii) **safe design requirements**. While the safe design requirements will apply to all services in scope, the minimum age will only apply to risky social media and video-sharing platforms.

2.1 The EU-wide minimum age for social media

Access of children to platforms remains a key issue and whether kids have or not an account makes a huge difference in terms of risks. With this in mind, the proposal sets an **EU-wide minimum age for minors to open an autonomous account at the age of 15** while ensuring a gradual approach. In particular:

For children aged 0 and below 3, there should be no access to social media or risky services. At this age, children are mainly exposed to relational risks as passive users of digital media. These risks often arise when parents and guardians replace direct interaction with screen use to soothe or distract young children, potentially affecting children's attention span, language, and vision development as well as socio-emotional growth. Caregivers should therefore prioritise face-to-face interactions, limit their own time on social media while caring for children and avoid exposing their children to screens.

For children aged 3 and below 13, parents can open fully parentcontrolled accounts on "childfriendly" services that meet strict safety standards appropriate to the child's developmental stage. This would cover specially designed child-friendly services within scope of the Regulation, provided they comply with the required safety by design criteria.

For children aged 13 and below 15, parents may set up introductory accounts for social media and video-sharing platforms that would be subject to the minimum age. These

⁸ The definition of parenthood will follow national legislation in each EU Member State.

accounts would have strictly limited features and be under parental control. Social media features would be limited to a maximum number of peer-only contacts and limited screen time per day. Parents and guardians would in addition be able to exercise their parental responsibilities by monitoring and controlling the use of the child's account via a dedicated guardian app.

As of 15 or older and below 18, the proposal proposes that teenagers in this age bracket can set up their own autonomous account on social media and video-sharing platforms, without the need for parental approval, while ensuring that this gives them access to an environment that is safe by design. During this period, the role of parents and guardians still remains essential.

2.2 Safe design

In addition to the measures outlined above, the EU KIDS Act obliges all services in scope to be designed safely by following strict rules and principles (dos and don'ts). This will ensure a safe experience that is age-appropriate. These are in particular:

- **No addictive design features**, such as infinite scrolling, artificial notification, or certain reward features.
- **Regulated recommender systems** such as options to choose, tune and control recommended content, avoid rabbit hole effects and go beyond engagement-based signals.
- **Safe account settings** to keep the content private, disable risky settings by default, and unambiguously inform minors.
- **No unwanted contacts from other users**. Unknown users cannot initiate direct contact outside of approved connections, explicit permission will be needed for being added to groups, easy and anonymous blocking.
- Enable children to **easily report harmful content** and access **support tools**.
- Offer effective and age-appropriate **parental control tools**.

These rules and principles will be complemented by tailored commitments for online games, AI chatbots and companions, offering a co-regulatory approach based on industry-led self-regulation. Software application stores would also be subject to requirements, building on current self-regulatory best practices. They would apply consistent age ratings and make apps, such as online games, inaccessible to minors below the rated age.

2.3 Age verification

The proposal also regulates **privacy-preserving and accessible age verification systems** and how they function. The EU KIDS Act will oblige providers of social media services and video-sharing platforms to **perform age verification when a user opens a new account**. This would be done by relying on the EU age verification tool or other solutions by public authorities that offer an equivalent level of accuracy, reliability, robustness, privacy, security, non-discrimination and non-intrusiveness. Existing accounts would be subject to proportionate checks rather than blanket age verification. This would be the case for instance if an account has been already created many years prior or combined with a credit card on the account holder. For online games specifically, **obligatory age recommendation** will be

required for every game with strict enforcement through age verification in a software application store upon download of the game.

In addition, in order for social media services not to get access to children before the safety design have been fully verified by public authorities, the proposal will foresee **verification of such services before they are made available to minors**.

EU
R
A
C
T
I
V

2.4 Enforcement

To ensure effective protection for children, strict enforcement is critical. The EU KIDS Act builds on the existing **enforcement architecture** from the DSA and the AI Act. The burden of proof to demonstrate compliance with new rules lies with the operators. This is why very large online platforms, or very large online search engines, will be obliged to submit a compliance plan to the Commission. The Commission shall assess within 30 days and the new service, feature or functionality can only be rolled out after positive opinion by the Commission. The Act also introduces a supervisory fee to effectively fund and support the Commission's EU-wide enforcement and supervision work. Within the enforcement structure, **priority will be given to complaints related to minors and stemming from minors**.

As technology moves rapidly, the proposal foresees a **review clause** to cater for the possible need of an update of the regulatory framework.

3. Complementary measures

3.1. Complementary EU regulatory measures

The EU KIDS Act will set out **specific rules** for the digital services, the use of which pose the highest risk to minors' **safety and development**. It focuses on a gradual access approach and on ensuring that certain design **features are safe by design**. At the same time, we need to ensure that minors' safety is **ensured** when it comes to all services and products that children can encounter online and that **commercial practices** that reach them are not posing risks to their health and safety.

The upcoming **Digital Fairness Act (DFA)** and the **revision** of the **Consumer Protection Cooperation Regulation** are a key opportunity to **embed the** protection of children and teenagers at the heart of EU consumer law. The DFA will **update** horizontal consumer protection rules against harmful commercial practices online that **also** affect children as young consumers, such as manipulative business-to-consumer **digital practices**, unfair pricing techniques, problematic influencer marketing and **issues** with digital contracts and subscriptions. The Commission will also revise the **Consumer Protection Cooperation Regulation** to ensure stronger enforcement of consumer law for **the benefit of all** consumers, including minors, and to provide a level playing field for compliant businesses. In preparing the revised Regulation, the Commission will consider ways to **improve enforcement** coordination between national consumer authorities in cross-border situations and centralise investigation and enforcement powers at EU level in specific cases.

In addition, the Commission will put forward the revision of the **Audiovisual Media Services Directive** which will specify the categories of harmful content that video sharing platforms must protect minors from. It will also clarify the applicability of EU audiovisual rules to influencers as providers of content.

Beyond the development of an appropriate regulatory framework and its effective enforcement, the Union response needs to rely on a range of support measures such as those outlined below.

3.2 Empowering children and young people through education

First, **education is key to fostering the development of every child**, equipping minors with adequate knowledge to better understand the online environment and enabling them to discern between appropriate and risky behaviours, including online. With this in mind, it is essential that young people are equipped with the skills they need to safely and responsibly engage with "Social Media+", including in the context of accelerated use of AI.

Against this background, the Commission will adopt an **Education package** to support schools in their efforts to promote digital and AI skills, raise awareness and build resilience among minors, **including through the preparation of teachers and school leaders**, on the impact of "Social Media+" on mental health and cognitive development. In this context, psychological support, as well as comprehensive age-appropriate education are key.

The forthcoming Education package will further **mainstream AI literacy education**, including **through the EU-OECD AI literacy framework for primary and secondary education**, and support schools in developing strategies to foster the digital wellbeing of children, focusing on their safety and empowerment. It will also address the supply of safe, interoperable European digital education infrastructure and pedagogically sound education content and help reduce Europe's strategic dependencies in educational technology.

The EU co-funded **Safer Internet Centres** already provide effective, trusted help to keep children safe online. Their national presence, wide reach and specialised expertise, make the network a valuable partner for Member States in developing and implementing effective national strategies for a safer and better digital environment for children. Building on this work, the Commission plans to provide **tailored guidance on the new rules** for different groups, including children, guardians, educators, schools, and regulators. This will include webinars, early detection of harm, managing age-appropriate access, and using AI chatbots and companions safely. Member States should build on this work and strengthen it in the national, regional and local context.

As concerns financing, under **Horizon Europe**, the Commission already funds research on child safety online. The work programme for 2026 includes the impact of the use of digital tools outside school and for communication on educational outcomes and mental health, with relevant projects starting in 2027. In addition, the Commission can identify **emerging research funding priorities**, as well as opportunities to support safe services and child-centred innovation with direct private and public-sector investment.

In parallel, action should be undertaken to **ensure children spend time in the offline world**. Through Erasmus+, the Commission supports offline spaces and activities, as they are crucial for the development of children, as they help promote healthy engagement and offer alternatives to screen use. It therefore encourages Member States to expand access to affordable sports, arts, youth clubs, libraries, and community spaces. EU Member States and regions should make full use of available national and EU funding, with a view to provide appropriate infrastructure for teachers, parents, and children.

These efforts should be part of a broader, strong collective commitment at both Union and national level to **mobilise all available resources for education, awareness raising and exchange of best practices**, with a view to strengthening prevention, support and protection mechanisms for children in the digital environment in an integrated approach to child protection. In this context, swift transposition and implementation of the Product Liability Directive will allow victims of defective products, including digital products, to claim compensation under uniform conditions throughout the EU.

3. Broader EU support measures

Besides education and media literacy, a number of further EU complementary measures are critical to address the protection of children online. These include a comprehensive approach to health, especially mental health, and better cooperation and coordination of those involved in addressing online risks and crimes against children.

In 2023, the Commission had already adopted a Communication on a comprehensive approach to mental health, including 20 flagship initiatives and almost EUR 1.3 billion in funding opportunities. The initiative put a greater focus on inclusiveness and supporting vulnerable groups, such as children and young people. The Commission is now developing, jointly with UNICEF, **a prevention toolkit** which will help policy-makers to better support the mental and physical health of children. The toolkit will be launched at the occasion of the World Mental Health Day, in October 2026. The toolkit will also address challenges in relation to the impact of digitalisation on children's mental health. In addition, the Commission is cooperating with the World Health Organization on **capacity-building in mental health systems** which also address digital determinants of youth mental health.

Children can also be victims of crime. Where children are affected by **criminal offences online**, as victims, perpetrators, or both, the EU procedural criminal law *acquis* applies, in particular the Victims' Rights Directive and the 2016 procedural safeguards Directive. When it comes to crime prevention, the substantive EU criminal law *acquis* is the applicable framework, including most notably the Child Sexual Abuse Directive.

Crimes affecting children online range from hate crime, trafficking in human beings, abuse and sexual exploitation to recruitment into organized crime and violent extremism or terrorism. EU and national authorities enforcing different legislation will keep cooperating and sharing information and data promptly, to allow for the highest level of protection of minors. The upcoming **Action plan to protect children from crime** will seek to provide a coherent and comprehensive response to the various risks faced by children in relation to crime, both online and offline. It will aim at minimising children's exposure to crime, at strengthening the capacity of law enforcement and other competent authorities to investigate and prosecute crimes affecting children, and it will focus on supporting children in their journeys through the national criminal justice schemes. **With the child-centered approach, the rights and best interest of the child will be at the core of all initiatives.**

3.4 International Cooperation

In line with the EU International Digital Strategy, the EU has so far worked with Australia, Brazil, Canada, Singapore, the United Kingdom and Japan to protect children online, shaped the G7 Common Set of Principles regarding minors online⁹. It has further contributed to discussions at multilateral level, including the United Nations¹⁰. Strengthening cooperation with our international partners remains a priority to effectively protect minors online. The introduction, via the EU KIDS Act, of an approach to mitigating the impact of artificial intelligence on children via chatbots and companions **strengthens the EU's right-based and risk-based approach to AI**, which is of interest to many partners around the world. In

⁹ Subsequently endorsed by Leaders from Brazil, Egypt, Kenya, India and South Korea.

¹⁰ G7 Common Set of Principles defining a safer and more secure digital space for minors.

general, a single approach to protecting children online across the EU will make this international cooperation more effective, by providing a strong reference point to engage with partners to achieve the objectives of this initiative.

3.5 Monitoring

It is important to continuously analyse the development of digital services for minors, their impact on minors, and the effects of the initiatives taken within the Union. **The Commission will regularly take stock of progress** with the support of stakeholders, including youth and children rights organisations, children, and parents' associations. It will monitor the impact and effectiveness of the package of measures linked to this Communication.

This monitoring will track the **effects and possible need to adjust the minimum age framework**, to establish a structured, regular data collection system to understand the lived online experience of minors across the EU. This framework will be grounded on child participation, notably through the EU Children's Participation Platform under the EU Strategy on the rights of the child and BIK+ (Better Internet for Kids+). It will draw on research, work under the DSA and by the EU Centre for Algorithmic Transparency, which tracks how child safety online, emerging technologies and usage patterns evolve.

The monitoring will focus in particular on impacts on youth's mental health. It will also capture the positive dimensions of children's online experiences, including whether and to what extent minors feel empowered and safe online, and how their screen time is distributed across different activities.

4. Conclusions and next steps

This Communication sets out a framework built on a clear conviction: technology companies bear the primary responsibility for making their products safe. **Parents, not algorithms, should be raising Europe's children.**

We must build a digital world where our **children can grow up free and secure**, protected by the values that Europe stands for. Europe needs to be the best place to grow up in, and the best place to grow old in. That is the standard against which this response should be judged.

The Special Panel has delivered the evidence. It is now for the Union's institutions, together with Member States, industry, civil society, schools and families to **deliver the change that children and parents across Europe are asking for** – a world designed with their well-being in mind.

The Commission will:

- Propose a **Digital Fairness Act**
- Propose the **revision of the Consumer Protection Cooperation (CPC) Regulation**
- Propose the revision of the **Audiovisual Media Services Directive**
- Present an **Action Plan on Protecting children from crime**
- Present an **Education package**