

Eurochild's reaction to the report of the Special Panel on child safety online

**The panel's response to the call to
rethink the business model of social
media to address risks for children**



Eurochild
Putting children at
the heart of Europe

September 2026

Eurochild's reaction to the report of the Special Panel on child safety online

Eurochild consistently contributes to discussions on children's rights in the digital environment. Throughout this work, we advocate for a child rights-based approach that pays particular attention to children in vulnerable situations. We have sought to move the public debate beyond the narrow question of whether children should be banned from social media and towards a more fundamental question: **why are children navigating digital environments that were not designed around their rights, developmental needs or best interests?**

We therefore welcome the publication of the report by the Co-Chairs of the Special Panel on Child Safety Online. The report is the result of a broad consultation process involving researchers, practitioners, children and youth representatives, civil society organisations, public authorities and industry. The report acknowledges that its analysis was informed by civil society and other specialists, while clarifying that the final recommendations remain the responsibility of the Co-Chairs.

Alongside our participation in the Panel, Eurochild has brought its position into the wider public and institutional debate, including through media engagement. We are pleased to see that many of the concerns raised by Eurochild, our members and children themselves have found a clear place in the final report.

The report adopts a notably comprehensive approach. It addresses platform responsibility, harmful business models and design features, safety by design and by default, privacy-preserving age assurance, children's participation, access to platform data, research, education, support for parents and investment in offline alternatives. It reflects the central message of Eurochild's position: **age restrictions alone will not protect children if the digital environment itself remains unsafe.**

Structured around the twin pillars of **protecting and empowering minors**, the report opens by defining the rapidly evolving "social media+" environment, before examining in **Chapter 1** how children's needs, capacities and vulnerabilities change across developmental stages; assessing in **Chapter 2** the evidence on content, contact, conduct, contract and cross-cutting risks; setting out in **Chapter 3** protective measures such as age restrictions, safety and privacy by design, provider accountability, age assurance and stronger enforcement; and exploring in **Chapter 4** how children can be empowered through participation, digital literacy, support for parents and educators, accessible remedies, research and investment in safe online and offline alternatives. What particularly stands out is that the report also provides a broad synthesis of existing research on how the digital environment affects children.

1. A developmental approach

One of the report's most valuable contributions is its developmental approach. It considers how children gradually become supervised users, active participants and, eventually, increasingly autonomous digital citizens.

For its overarching recommendations, the report groups minors into three age ranges:

- **0-2 years:** screens and social media should generally be avoided. Children under three are primarily passive users affected by caregiver practices, screen exposure and “technoference”- situations in which digital devices interrupt or replace responsive interaction between children and caregivers.
- **3-12 years:** children should use only age-appropriate devices and “social media+” services, under appropriate adult supervision.
- **13-18 years:** adolescents should progressively develop greater autonomy in their use of age-appropriate digital services, while continuing to benefit from strong protections, safety-by-design measures and support adapted to their evolving capacities.

Its underlying developmental analysis is more granular, however, distinguishing between children aged 3-5, 6-9 and 10-12, as well as adolescents aged 13–15 and 16–18.

The report also recognises that the transition towards greater autonomy is a normal and necessary part of adolescence. The goal should be to create conditions in which they can develop autonomy without being exposed to systems designed to exploit developmental sensitivities, social pressure or incomplete self-regulation. Children should progressively be able to exercise their rights to information, expression, association, participation, play and education. **At the same time, platforms cannot use evolving autonomy as an excuse to withdraw safeguards from teenagers.**

2. Recognising different sources of vulnerability

The report also highlights that while all children are still developing, they are not all exposed to the same risks, nor do they have the same resources with which to respond. It identifies gender, socioeconomic background, racial and ethnic origin, religion, migration background, special educational needs, disability and pre-existing mental-health difficulties as factors that can influence exposure to online harm. It also recognises that these factors intersect and may compound one another.

This reflects a central component of Eurochild's position. Children experiencing poverty may have less access to high-quality devices, digital literacy, parental support and safe offline activities. Children with disabilities or special educational needs may be disproportionately exposed to grooming, harassment, hate speech and cyberbullying. Children belonging to minority groups may encounter discriminatory content or biased moderation systems. LGBTQI+ children and children who feel isolated offline may depend more heavily on online

communities for identity, belonging and support, even while facing particular forms of abuse within those same spaces.

Vulnerability is shaped by the interaction among a child's developmental stage, personal situation, social environment, and the design of the service they use. We must make those environments safer and more inclusive, while ensuring targeted assistance is available to children who face disproportionate risks.

3. Moving beyond social media through a “social media+” approach

We welcome the report's shift from a narrow definition of social media to what it calls the **“social media+” environment**.

The report recognises that risks arise from particular functionalities, designs, commercial systems and patterns of interaction. Its definition, therefore, covers not only social media platforms but also app stores, video-sharing platforms, gaming services, AI companions, and other digital services that contain risky features that are not age-appropriate. These may include infinite scroll, autoplay, recommendation systems, persistent notifications, harmful commercial practices and opportunities for dangerous contact. This aligns closely with Eurochild's call for a technology-neutral, **risk-based approach**.

The “social media+” approach is particularly relevant as platforms increasingly combine social networking, entertainment, shopping, private communication, gaming, advertising and artificial intelligence within a single service. Regulation must therefore follow the features and risks rather than relying exclusively on categories that quickly become outdated.

4. Understanding how children use digital services

Another valuable aspect of the report is its recognition that the consequences of digital use cannot be assessed only by counting the number of hours a child spends online. The **nature, purpose and context of use** also matter.

The report distinguishes between passive use - such as prolonged browsing or scrolling - and active use, including messaging, posting, commenting and interacting with supportive communities. It notes that passive consumption may be associated with loneliness, stress and depressive symptoms, while some forms of active engagement can contribute to social support, life satisfaction and connection. At the same time, it acknowledges that the evidence is mixed and that active interaction can also expose children to cyberbullying, harassment, grooming and harmful social comparison.

5. Risks to physical and mental health, emotional regulation and developmental displacement

The report provides substantial attention to the effects of digital use on sleep, attention, self-regulation, children's health (including mental health), and child development.

For very young children, increased screen exposure is associated with shorter sleep, disrupted caregiver-child interaction and dysregulated stress patterns. Because young children are still developing mechanisms of emotional and behavioural self-regulation, highly stimulating digital environments may be particularly difficult for them to manage. The report also emphasises that, in early childhood, digital harm may arise not only from content but from the replacement of interaction, play, language exchange and attentive caregiving. **The report also notes that in its most serious forms, the displacement of caregiver interactions may equate to 'digital neglect'.**

For older children and adolescents, the report highlights the displacement of sleep, outdoor activity, face-to-face relationships and other developmentally important experiences. It notes that evening screen use can delay sleep, provide psychological stimulation and interfere with sleep quality. The effects differ by age: children aged 6-12 may experience longer sleep latency and poorer-quality sleep, while adolescents aged 13-15 may experience delayed sleep onset, reduced sleep quality and heightened cognitive arousal before sleep.

These findings show why attention-capturing design cannot be treated as a neutral consumer choice. When autoplay, notifications, recommender systems and infinite scroll are deliberately designed to prolong engagement, the consequences extend beyond the screen. They can affect sleep, concentration, learning, emotional regulation, relationships, physical activity and the time available for creativity and play.

6. The 5Cs framework

We particularly welcome the report's incorporation of the **5Cs framework**, which Eurochild recommended as a basis for more comprehensive risk assessments. The framework categorises risks as content, contact, conduct, contract and cross-cutting risks.

This matters because public discussions often focus almost exclusively on harmful content. Content is only one component of children's digital experiences. Harm can also arise from who contacts a child, how children are encouraged to behave, the commercial conditions they are drawn into, how their data are used, and how design systems affect their health and autonomy.

The 5Cs framework therefore provides a much stronger basis for assessing services than simply asking whether individual posts or videos are illegal. It allows policymakers to examine the architecture of a service, its revenue model, communication features, purchasing systems, recommendation mechanisms and broader consequences for children's rights.

Eurochild called for the 5Cs to be embedded systematically in mandatory, detailed and independent risk-assessment templates covering all relevant digital environments. For this purpose, it would be important to establish a binding assessment procedure or an independent European body to apply it to individual services.

7. Making providers prove that their services are safe

The report proposes a potentially transformative principle: **the burden of proof should shift to providers.** This represents an important change in regulatory logic. Currently, digital services are generally launched and used by children before authorities have established whether their design is developmentally appropriate. Regulators, researchers, civil society and affected families may then have to gather evidence of harm after the product is already widely used.

The report itself highlights this inconsistency by contrasting digital services with sectors in which products used by children are subject to safety requirements before entering the market. Its burden-of-proof recommendation leans toward the independent, preventive approach advocated by Eurochild.

However, the institutional mechanism remains unclear. **Who determines that a service is safe? Against what criteria? How frequently is the assessment repeated? What evidence must a company provide? Can the service operate while an assessment is disputed?**

Eurochild calls for detailed risk-assessment templates developed by an independent European body, the systematic use of the 5Cs, child-impact audits, and minimum criteria that services must meet to operate or be accessible to particular age groups.

The Digital Services Act represents major progress, but its systemic-risk regime under Article 34 applies specifically to designated Very Large Online Platforms and Very Large Online Search Engines. Providers carry out the initial risk assessments themselves.

The report's burden-of-proof proposal could therefore fill a significant gap, but only if it is accompanied by genuinely independent assessment and enforceable pre-access or pre-market criteria. Otherwise, "providers must demonstrate safety" risks remaining an important principle without a sufficiently clear decision-making structure.

8. Shifting responsibility away from children and parents

The report clearly states that providers retain primary responsibility for the safety of their products. Eurochild has consistently argued that it is neither fair nor realistic to expect children and parents to "self-manage" platforms deliberately designed to make disengagement difficult. Media literacy, parental support and individual resilience are important, but they cannot compensate for unsafe products or business models.

The report reflects this position clearly. **Its guiding principles state that protection from harmful content and addictive features, and violations of children's rights online, should**

be built into the design of digital services. It calls for rules addressing infinite scroll, autoplay, push notifications, dark patterns, unsolicited contact, rabbit holes and problematic personalised recommendation engines. Protective settings should be the default, not an option that children or parents must locate and activate.

This closely mirrors Eurochild's call to reduce harm at source by tackling the underlying business model. Our position calls for restrictions on profiling, targeting, and opaque recommender systems; the elimination of manipulative design; and the introduction of independent child-impact assessments. It also stresses that children's identities, behaviour and attention must not be treated as commercial assets.

The report recognises the role of the "attention economy" and the use of engagement-maximising systems. It therefore moves the discussion beyond individual content moderation and towards structural accountability. This is a significant step forward.

The report recognises harmful commercial practices and recommends stronger consumer protection for minors. It also calls for children's best interests to be a primary consideration when their data are processed under the GDPR and for children to be equipped to recognise practices such as targeted advertising.

9. Age assurance and children's rights to privacy

The report states that age-verification or age-estimation methods must be proportionate, accurate, robust, inclusive, non-discriminatory and easy to use. They should uphold children's fundamental rights and the highest standards of privacy and data protection. The report specifically warns against using identity documents or biometric data for age estimation. **It supports zero-knowledge-proof systems that allow a user to demonstrate an age attribute without being identified or tracked.**

This is strongly aligned with Eurochild's view that age assurance must never become a new instrument for profiling or commercial data collection. Its function should be strictly limited to confirming whether a user falls above or below a relevant threshold. It must operate alongside wider safety measures and cannot substitute for platform responsibility.

The report likewise links age assurance to safety-by-design and age-appropriate experiences rather than presenting it as a standalone technical fix. That is an important safeguard. Knowing a user's age does not make harmful recommender systems, manipulative interfaces or exploitative commercial practices safe.

The report recognises that very young children cannot consent to their digital representation or understand the future and commercial consequences of having their lives documented online. Importantly, the report states that platforms should not incentivise the creation and dissemination of content featuring children through monetisation, algorithmic amplification or engagement-driven design. This closely reflects Eurochild's call to address sharenting and child influencers through enforceable platform obligations rather than relying exclusively on individual parental responsibility.

10. A comprehensive legislative approach

The report reflects Eurochild's insistence that online child safety requires a coherent approach across several areas of EU law. It examines the Digital Services Act, the General Data Protection Regulation, the Audiovisual Media Services Directive, the Artificial Intelligence Act, consumer protection legislation, and product liability rules. It also considers the forthcoming Digital Fairness Act, child sexual abuse legislation, cyberbullying, criminal law measures, and the need for stronger cooperation among different enforcement authorities.

The report also supports the swift adoption of measures to prevent, detect, report and block child sexual abuse online, including within interpersonal communications. Social-media restrictions cannot address grooming, sexual exploitation and abuse occurring across messaging, gaming and other digital services.

Importantly, the report recognises that having legislation on paper is not enough. Enforcement authorities require adequate expertise, staff, resources and cooperation. It also calls for a stronger role for civil society in enforcement, including through existing structures and by contributing to enforcement capacity. This is complemented by recommendations for sustained public funding and common standards for Safer Internet Centres and comparable civil society organisations, including for awareness-raising, training, support services, helplines and capacity-building.

11. Research, platform data and the limits of current evidence

The report gives considerable attention to gaps in the evidence base. It acknowledges that much research on social media and mental health is correlational and cannot, on its own, demonstrate causation. **At the same time, it concludes that the available evidence provides sufficient indications to justify precautionary action.**

The report calls for long-term European longitudinal research, randomised controlled trials where appropriate, independent academic involvement in risk-mitigation design and secure European research infrastructure. It also calls for stronger enforcement of researcher access under Article 40 of the DSA. It recognises that the quality, continuity and scope of platform data will determine whether independent scrutiny is meaningful.

This closely reflects Eurochild's position that researchers need access to objective platform data rather than relying on selective disclosures, company-funded studies or public-relations materials. We also called for interdisciplinary research that combines developmental, psychological, sociological, and, where appropriate, neuroscientific evidence, as well as children's own experiences.

More attention is still needed to populations that remain underrepresented in research. Eurochild therefore continues to emphasise and support the need for evidence concerning children experiencing poverty, children in alternative care, children with disabilities, children from migrant and minority backgrounds, and children living in different geographic and

cultural contexts. Research based mainly on relatively advantaged populations cannot automatically be assumed to describe the experiences of all children.

12. Digital opportunities, participation and offline alternatives

The report recognises that safe digital services can support learning, creativity, communication, civic engagement, identity development, and access to peer support. It calls for children to participate meaningfully in the design of policies, safety measures, educational initiatives and evaluations, with particular efforts to include children from disadvantaged and marginalised groups.

Children must be protected, but they must also be heard. Policies developed without children risk misunderstanding how services are used, why children value them, how restrictions are circumvented and what safer alternatives would actually meet their needs.

The report also takes public authorities' responsibility seriously and calls for alternatives outside commercial platforms. It recommends investment in affordable sports, arts, youth clubs, libraries, and community spaces where children can connect, learn, and play. It also calls for public funding for civil society, peer counselling, helplines, education, parental guidance and mental-health services.

This reflects Eurochild's argument that states cannot outsource their obligations under the UN Convention on the Rights of the Child to private companies. For some children, social media has filled a vacuum created by the absence of safe community spaces, youth services, mental-health support or meaningful opportunities for participation. The response cannot simply be to remove access without addressing that vacuum.

The Special Panel report recommends a harmonised EU-wide restriction below the age of 13 across the broad "social media+" category, with limited access under parental supervision or in educational contexts. It also leaves Member States the option to adopt additional precautionary measures for adolescents over 13.

At the same time, the report makes clear that restrictions should be precautionary rather than permanent and that the ultimate objective is for providers to make their services safe and age-appropriate. **Its most important contribution may therefore be not the specific age of 13, but the principle that access restrictions should pressure companies to change their products rather than absolve them of responsibility.**

The report argues that access restrictions should remain in place until providers demonstrate that their services include safe, age-appropriate features. Where a safe-by-default version exists, adult or otherwise inappropriate functions should only become available after effective age assurance.

A strong basis for the next stage of EU action

Overall, the Special Panel report represents a substantial step towards the approach Eurochild advocates for. It recognises that online safety is about platform architecture, data exploitation, recommender systems, commercial manipulation, developmental needs, inequality, public services and corporate accountability.

The report nevertheless leaves essential implementation questions unresolved. **The EU still needs a credible method for determining whether specific features and services are genuinely safe, independent of the provider's own assessment.** It needs clear standards applicable beyond the largest platforms, robust child-impact assessment, universal protection for children who circumvent restrictions or access services without logging in, and stronger rules addressing the commercial use of children's data and identities.

The next stage of the debate should focus on the conditions platforms must meet before they are permitted to reach children.

That is the central message of Eurochild's position: **platforms should have to prove that the environments they create respect children's rights.**

For more information, contact:

Francesca Pisanu
EU Advocacy Officer
Francesca.pisanu@eurochild.org

Eurochild AISBL

Avenue des Arts 7/8, 1210 Brussels
Tel. +32 (0)2 511 70 83
info@eurochild.org

© Eurochild 2026