

# Joint statement from the EU Coalition for Children's Right Online<sup>1</sup> on the EU KIDS Act Proposal

29 October 2026

The proposal for an EU Keeping Internet Digital Spaces Accountable and Trustworthy Act (EU KIDS Act) introduces new binding rules on the protection of minors in the digital environment. **The Coalition for Children's Rights Online welcomes this development as an opportunity for a landmark framework that makes digital services safer for children**, notably by reducing their exposure to harmful and addictive design.

As a collective of human rights and children's rights organisations, we commend the proposal's grounding in fundamental rights, including children's rights, as recognised by the Charter on Fundamental Rights.<sup>2</sup> We also strongly support the precautionary approach, that establishes default safety-by-design principles for all minors and new due diligence obligations on specific providers.

**However, to realise the promise of a safer digital environment for all children and honour the commitment to reverse the burden of proof, requiring platforms to prove that they are safe,**<sup>3</sup> we recommend embedding the following principles more firmly in the proposed Regulation:

- **Greater recognition of diversity of children's lived experiences and of unequal risks and exposure** to online harms. These differentiated experiences depend on many factors,<sup>4</sup> including socio-economic backgrounds, which also influence the resources and capacities parents and guardians possess to support their children online.
- **A strict implementation of the principle of accountability**, requiring providers to ensure the safety and privacy of their services through default protections, without placing too much burden on parents and relying on guardian tools.
- **A greater tech neutral approach through streamlined obligations and safety requirements for services**, which should be based on the level of risks depending on the

---

<sup>1</sup> This document aims to support the work of the European Parliament and the Member States on the EU KIDS Act's proposal. It is not exhaustive and does not represent the final contribution of the signatories.

<sup>2</sup> [Charter of Fundamental Rights of the European Union](#). (2000). Recital 74.

<sup>3</sup> [State of the Union Address by President von der Leyen](#). (2026).

<sup>4</sup> Notably their age, gender identity, sexual orientation, migration status, disability status, family type, or any other circumstances and conditions, such as children living in institutions, children that are victims of abuse. See also [Special panel report on child safety online](#). (2026). Chapter 2.

cumulative effects of features and functionalities, rather than on the type of service. In its current form, the risk classification is underdeveloped, and the proposal contains too many exceptions, which could create loopholes and expose children to great risk.

- **A strengthened ex-ante approach through risk assessments and a pre-certification process for all services accessible to children.** This would shift the burden onto providers to demonstrate proof of safety through an independent process and would also establish a sustainable and future-proof framework for addressing emerging technologies and new risks.

To implement these principles and ensure that the Regulation leads to an EU-harmonised framework that would protect and empower all children in Europe, we suggest these first main changes to the proposal:

### **1. Cover every service that is accessible to minors and may cause them harm**

We welcome a scope that reaches beyond social media and video-sharing platforms (VSPs) to AI chatbots and companions, online games, and software application stores, and that includes small and micro enterprises. However, the proposal still defines obligations depending on the type and size of a service rather than by the risk it poses. Services offering the same risky features, such as contact from unknown adults on gaming platforms or engagement-driven design in AI chatbots, can be as harmful to children as social media, and technologies that emerge after adoption would fall outside the Regulation altogether. In addition, the exemption for education technologies<sup>5</sup> covers any service designed primarily for educational purposes and operated by, or on behalf of, an educational establishment. This definition is too broad and could shield services that are harmful to children.

### **Recommendations**

- a) Broaden the scope to all digital services that are accessible to minors and may cause them harm, including to their physical, psychological and social wellbeing, defined by the risks of their features and functionalities rather than by service category.
- b) Introduce a proportionate and independent risk assessment obligation to identify the services that must comply with the Regulation, so that new and emerging services are covered without reopening the text.
- c) Narrow the education technology exemption to services that have demonstrated a very low risk to minors.

---

<sup>5</sup> [EU KIDS Act](#), Art.2.4(c). (2026).

## **2. Guarantee the same level of protection wherever children are online**

The dedicated, binding safety-by-design framework is the most important achievement of the proposal. It enshrines the Guidelines on the protection of minors in hard law, makes providers responsible by default for the safety, privacy, and security of all minors up to 18, and prohibits the most dangerous features. However, the level of protection is uneven between services. For online games, protection against commercial risks appears in the Recitals but not in the obligations,<sup>6</sup> while obligations regarding contacts and interactions safeguards are weaker.<sup>7</sup> For AI chatbots and companions, the rules on addictive design are less complete than for social media and VSPs,<sup>8</sup> and smaller providers are exempted from post-market monitoring. For both AI systems and online games, adherence to a voluntary code of conduct is presumed enough to demonstrate compliance.<sup>9</sup> Finally, some protections, notably on other commercial risks, content moderation, and search functions, are not covered at all.

### **Recommendations**

- a) Align the obligations on commercial practices and addictive design across all services in scope, starting by extending the protections on economic transactions to online games.
- b) Strengthen and complete the obligations on AI chatbots and companions,<sup>10</sup> and require post-market monitoring from providers of all sizes.
- c) Ensure that compliance rests on binding obligations: codes of conduct can support implementation but must not create a presumption of compliance.
- d) Ensure that no safeguard contained in the Guidelines is lost, including identified gaps such as content moderation, broader interactions,<sup>11</sup> search functions, virtual rewards, etc.
- e) Extend obligations on commercial transactions beyond the transparency of the transaction to cover manipulative design and other risky features (hidden or harmful advertisement, content monetisation, marketplaces embedded on social media, etc.).

## **3. Make access depend on the safety of the service, not on parents**

---

<sup>6</sup> [EU KIDS Act](#), Recital 40 and Art.15. (2026).

<sup>7</sup> [EU KIDS Act](#), Art 12.2 on manipulating minors into approving direct contacts and Art 13 (a, b, d, e, f) on the visibility of content shared by minors do not apply to online games. (2026).

<sup>8</sup> The EU KIDS Act Art. 9(2) does not apply to AI chatbots and companions, while some features (notifications, reward, incentivising engagements) might also be implemented on these services.

<sup>9</sup> [EU KIDS Act](#), Art. 14.3 and 15.4. (2026).

<sup>10</sup> Notably regarding persuasive design (notifications, features that incentivise engagements,...), recommender systems (exposure to information that may pose risk to their privacy, safety, and security, information based on the collection of personal data outside of the service, or on implicit engagement-based signals), input and output classifiers for illegal content, and regarding commercial nudging of embedded advertisement.

<sup>11</sup> Such as tags, comments, reports, mentions, etc.

We welcome harmonised age limits across the EU to avoid diverging national thresholds and an uneven level of protection, and the choice of 13 as the first age of access, as recommended by the Special Panel, many experts, and child and youth representatives. However, the proposed rules differ between categories of services, and access below the age limit rests on guardians. Children under 13 can use AI chatbots, companions, and online games through guardian tools, while children between 13 and 15 can use social media and VSPs only through a parent-supervised account. Access is therefore conditional on parental consent rather than on whether the service meets the safety standards of the Regulation. This leaves guardians to judge whether a service is safe, creates inequalities between children depending on the resources, availabilities, and capacities of their families, and puts the most vulnerable children at greater risk.

## Recommendations

- a) Harmonise the age limit at 13 for all risky services: social media, VSPs, AI chatbots and companions, and online gaming platforms containing similar risky features.
- b) Replace the parent-supervised accounts for children between 13 and 15 with specific default protections appropriate for this age group, built into the service and applicable to every child regardless of parental involvement.
- c) For other services, determine the appropriate default protections and safeguards through the risk assessment process, in line with children's evolving capacities.

### 4. Make guardian tools a support for children and their families

Beyond access, the proposal places too much burden on parents and guardians<sup>12</sup> across the whole safety framework, as the tools for guardians must include mechanisms to manage time limits, safe settings, contact and interaction safeguards, report content, accounts, and groups.<sup>13</sup> Key safety and reporting mechanisms once again depend on the guardian's resources and digital skills, rather than on the architecture of the service. This departs from the principle that tools for guardians are complementary to safety by design and by default<sup>14</sup> and must support children and their families. Regarding the technical tools themselves, some conditions are set in the proposal, notably on transparency to the child,<sup>15</sup> but it remains unclear how they will be implemented. In addition, there is a lack of clarity on how the wider ecosystem of actors needed to protect and empower minors in the online environment will be supported.<sup>16</sup>

---

<sup>12</sup> The definition of guardians should also accommodate legally authorised institutions, bodies, and professional exercising parental responsibilities

<sup>13</sup> [EU KIDS Act](#), Art. 20(4) and 20(3). (2026).

<sup>14</sup> [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](#), §80. (2025).

<sup>15</sup> [EU KIDS Act](#), Art. 20 (1) and (2). (2026).

<sup>16</sup> [EU KIDS Act](#), Art 33 of the proposed regulation. (2026). See also [Special panel report on child safety online \(p. 8\)](#). (2026).

## Recommendations

- a) Ensure that safety settings, safeguards,<sup>17</sup> and reporting mechanisms are activated by default and directly accessible to minors.
- b) Provide optional, interoperable, and privacy-preserving guardians support tools as a complement to these default protections.
- c) Require that these tools focus on support; are transparent, proportionate, and responsive to children's needs and evolving capacities; and preserve confidential access to helplines and support services.
- d) Strengthen the requirements for measures at the EU and national levels to protect and support minors and their communities, building on the experience of the Safer Internet Centers, family and mental health organisations and helplines.

### **5. Require proof of safety before access to the market**

We support the new due diligence obligations, which begin to reverse the burden of proof: very large online platforms must submit a compliance plan audited by independent experts,<sup>18</sup> and providers of AI chatbots and companions must evaluate risks before placing their systems on the market.<sup>19</sup> However, these ex-ante requirements reach only some providers. There is no pre-certification process or safety label for other services, no independent body to assess whether a service respects the safety requirements, and the role and composition of the Child Safety Committee<sup>20</sup> remain unclear. Without independent verification before accessing the EU market, the Regulation cannot deliver on the commitment of reversing the burden of proof, and it gives providers no incentive to build services that are safe for everyone. It also fails to provide a process that will cover emerging technologies and new features and functionalities, and therefore, fails to make the proposal sustainable and future-proof.

## Recommendations

- a) Introduce a pre-certification process, based on an independent risk assessment, for all services in scope, proportionate to the size and the level of risk of the service.
- b) Give the Child Safety Committee a stronger role, with a clear mandate and composition, in both the risk assessment and the pre-certification processes.
- c) Lift age restrictions for services certified as safe for all users, creating a real incentive for providers to design safe services.

---

<sup>17</sup> Including access to child helplines.

<sup>18</sup> [EU KIDS Act](#), Art.5. (2026).

<sup>19</sup> [EU KIDS Act](#), Art. 14 (2026).

<sup>20</sup> [EU KIDS Act](#), Art 40. (2026).

Building on the Digital Services Act, General Data Protection Regulation, AI Act, and consumer law—whose effective enforcement remains essential—and alongside the forthcoming Digital Fairness Act, the EU KIDS Act offers a clear opportunity to address harmful design and commercial practices. If implemented by default and through ex-ante processes, the safety and privacy requirements could ensure that children’s rights online do not depend on their family’s resources or access to guardian support. It could lead to the possibility for teenagers to participate in a safer digital environment, while younger children (under 13) would access services that have been designed specifically for them.

We remain fully committed to dialogue and look forward to engaging closely throughout the negotiation process to ensure that the proposed Regulation delivers a rights-respecting, robust, enforceable, and future-proof framework for the safety of all children.

## **Signatory organisations:**

5Rights Foundation  
Børns Vilkår  
Center for Countering Digital Harm  
Child Focus  
Child Helpline International  
ChildFund Alliance  
Children's Rights Alliance  
COFACE Families Europe  
CyberSafeKids  
ECPAT International  
Eurochild  
European Youth Forum (YFJ)  
Internet Watch Foundation  
Mental Health Europe  
Missing Children Europe  
SOS Children's Villages Denmark  
SOS Children's Villages International  
Terre des Hommes Netherlands  
Vlaamse Jeugdraad (Flemish Youth Council)