

Eurochild response to European Commission call for evidence on Guidelines to enforce the protection of minors online

About Eurochild

Eurochild is one of the leading child rights networks in Europe, representing over 200 child rights organisations in 42 countries. We work to put children's rights at the core of EU and national policymaking, to ensure children's rights are implemented both offline and online, on the basis of the United Nations Convention on the Rights of the Child (UNCRC). We focus on influencing policies and practices to improve the lives of children, especially those from vulnerable backgrounds. Overall, Eurochild plays a significant role in advancing children's rights in Europe by connecting organizations, and ensuring that children's voices are heard in decision-making processes.

Introductory remarks

We welcome the European Commission's work on guidelines to enforce the protection of minors online as part of the Digital Services Act, as it has big potential to advance in the guarantee of children's rights online. Particularly important is the aim of the European Commission to consult different actors, including children, in the drafting process.

With this submission Eurochild contributes to the European Commission call for evidence launched with reference Ares(2024)5538916 on 31 July 2024. Attached we include a statement signed by 34 child rights organisations with key asks on the guidelines.

According to our [latest research on online safety](#), children are aware of online risks and generally support online safety measures. The main concerns expressed by participating children were:

- **cyberbullying** and harassment;
- data and **information security** (including the misuse of the pictures and videos they share online by other users, especially in the context of child sexual abuse related harms);
- viewing inappropriate content;
- being **contacted by unknown people**, especially for child sexual abuse related harms.

Related to all these, they were especially worried about the consequences on their physical and **mental health** (addiction, isolation, anxiety, mood disorders). Children said to use proactive strategies for self-protection online, denoting a high level of self-imposed responsibility for their own online safety, namely: (1) self-awareness and self-censoring; (2) in-app blocking and reporting features, although acknowledging their low effectiveness. Talking to caregivers proved to be difficult for many children in the study and seeking in-person support was mostly considered only for the most serious harms.

They emphasized that online safety measures should prioritise their protection without compromising their privacy, leaning towards safety-by-design approaches. Children expressed a strong preference for **online safety measures that promote user agency**, for instance, providing child-friendly information, optional safety and privacy settings, optionally blocking sensitive content or meaningful pop-up warnings. In parallel, the guidelines should set minimum safety- and privacy-by-design baselines that all online services providers must respect, prioritising the responsibility and accountability of online platforms to protect children.

Another characteristic of empowering safety features is that they ensure children can make *informed* decisions on the level of protection and intrusiveness, by providing them with **age appropriate information** of the consequences and conditions of each setting/decision. For this, participating children suggested involving children themselves in making information about complex safety privacy settings more age-appropriate and accessible to make sure children can make informed choices online. The guidelines should provide that online platforms accessible to minors provide their Terms and Conditions, as per recital 46, and other features (i.e., reporting guidelines and features, safety and privacy settings, sensitive content warnings, etc.) in age-appropriate language.

Children also demanded to be involved in the *design* of such measures, arguing that it would facilitate efficient measures tailored to their needs while providing them with more agency. The guidelines should encourage online platforms to meaningfully involve children in the design of their online safety tools.

A risk- and child rights-based approach to assessing the provision of high level of safety, security and privacy to children

The main goal of the guidelines should be to support online platforms' compliance of the DSA's provisions to protect children in their services. In consequence, the guidelines must be **future-proof** and adaptable to an evolving technological landscape. It is important to note the need for a balanced structure of the guidelines between harmonised principles and platform specificity to ensure effectiveness while easing compliance across the different platform services. This includes **avoiding a long list of good practice difficult to be applied or scaled up across the industry** and the assumption that one measure that has proved effective in mitigating a specific risk in a specific platform provides automatic compliance to other platforms that may apply it.

In turn, the guidelines should **provide a framework to help platforms ask the right questions**, notably to assess if they are likely to be accessed by children, and if so if they provide a high level of privacy, safety and security, namely through a **child rights impact assessment**. Such assessment should also be accompanied by good practice and recommendations for mitigation measures.

An approach based on children's rights is justified both by the evolving nature of the digital environment and the online risks and by the complexity of the risks aimed to be addressed by this instrument. The 'Child Impact Assessment' proposed by the guidelines shall not be done on the basis of specific features or risks (as outlined in the European Commission's call for evidence), but rather **focusing on the effect of design choices in the exercise of children's rights**, as outlined in the UN Convention on the Rights of the Child. This will ensure not only that the guidelines are future-proof but also that the assessment effectively leads to measures that will both protect and empower children, in line with the approach of the Better Internet for Kids+ Strategy. Such an assessment should include questions around:

- Is your service accessible to children? How do children use your service and what risks are associated with that use? (Right to access)
- Do you measure your platform algorithms' discriminatory and abusive effects against children, if any? What mitigation measures do you have in place? (Right to non-discrimination)
- Do you use age appropriate and accessible communications directed at children throughout their user experience? (Right to information)
- Are your design choices contributing to creating a safe and healthy environment for children and promoting healthy behaviors by and towards children? (Right to life, survival and development/Right to be protected from violence, abuse and neglect)
- Does your service collect children's data respecting children's right to privacy? (Right to privacy)

- Does your service help children recognize and understand commercial activities? (Right to be protected from all forms of exploitation)
- Do you make sustainable business decisions that consider the long-term effects of your service on children's development? Do you prioritise the best interests of the child? (Best interests of the child)
- Are you meaningfully listening to and respecting children's views when designing and reviewing your services? (Right to be heard)

The guidelines should also provide that, as this assessment identifies areas of improvement, online service providers look for modifications or alternatives to **mitigate potentially negative impacts**. For instance, in accordance with such an assessment (i.e., by incorporating the [BIK+ Self-assessment tool on age assurance](#)), the guidelines should provide that *appropriate* age assurance be in place for platforms that do not ensure a high level of privacy, safety and security.

The assessment tool provided by the guidelines should be **outcome based**, guiding the companies in what 'good looks like' and then **suggesting good practice and specific recommendations**. Such examples should include guidance on applying more granular analysis – including considerations of age, local contexts, etc., allowing for flexibility and adaptability to different types of platforms and services. Finally, the guidelines must encourage online platforms to involve children when gathering data for the assessment included above.

Consultation with children

It is of outmost importance that the **drafting, implementation and monitoring of the guidelines is informed with children's views**, to ensure the implementation of the UNCRC and the Charter of Fundamental Rights (Article 24) and to ensure they will provide tailored and effective solutions to children's needs.

On the European Commission's guidelines on DSA Article 28(1)

Together with the 34 undersigning organisations and experts from all over Europe, we welcome the European Commission's work on guidelines on Article 28(1) of the Digital Services Act (DSA) requiring platforms accessible to children to "put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors". We thus present these minimum principles and elements that the guidelines should consider and include.

The guidelines are key for DSA implementation and enforcement. To protect and promote children's rights, they should **provide clear and concrete guidance to online platforms on how to comply with their obligations, as well as support Digital Service Coordinators in the coherent and coordinated application of article 28(1) at national level. The guidelines should be developed with the meaningful participation of children, and be based on principles and provisions of the UNCRC and guidance form General comment No. 25 on children's rights in the digital environment**, as well as existing frameworks like the Irish Fundamentals for a Child-Oriented Approach to Data Processing, the Dutch Children's Code, the Swedish guide on rights of children and young people on digital platforms, the CNIL Recommendations, the ICO's Children's Code, or the concept of personal integrity of minors in the German Youth Protection Act, as well best practices and highest available standards like CEN-CENELEC Workshop Agreement 18016 Age appropriate digital services framework, among others.

Based on such instruments and principles, the guidelines should **provide guidance for companies to ensure a high level of privacy, safety and security**, and notably:

- Provide a framework to help platforms ask the right questions, notably to assess if they are likely to be accessed by children, and how to evaluate with a **child rights impact assessment** if they provide a high level of privacy, safety and security for children.
- Provide that, based on that assessment, privacy-preserving, proportionate, effective, inclusive, age appropriate and secure **age assurance** is in place for platforms that do not to ensure a high level of privacy, safety and security for children, by design and default.
- Provide guidance on **measures and features** to achieve that high level of privacy, safety and security, addressing as a minimum the following elements.
 - Prioritising the best interests of the child when designing and developing services;
 - Avoiding persuasive design techniques such as intermittent reward systems, gambling-like features or endless scrolls;
 - Ensure data minimisation so that children's data is not unduly collected, disclosed, reused or shared;
 - Ensuring default high privacy and security settings, including limiting exposure of children's accounts to harmful contacts and content as well as removing illegal ones;
 - Providing log-in functionalities/authentication mechanisms in line with a child's capabilities;
 - Provide transparent, fair, age appropriate, and effectively applied and enforced terms and conditions, including effective content moderation;
 - Avoiding uses of data that may be detrimental to children's rights or in any way unlawful, as well as profiling, recommender systems, dark patterns and nudging;
 - Ensuring potentially problematic functionalities such as geolocation, microphone and camera are off-by-default;
 - Providing privacy-preserving parental controls in line all with children's rights;
 - Providing age-appropriate and effective reporting and redress mechanisms.

- Recommend that companies put in place **specific functions, roles and responsibilities dedicated to the protection and participation of minors**, to ensure that actions and measures are coordinated, carried out and evaluated based on adequate children’s rights expertise.
- Provide that companies re-assess and evaluate their compliance to the guidelines regularly, recommending them to do so with the meaningful participation of children.

In addition, the guidelines should recommend to regulators **measures to ensure the prioritisation of children’s rights in their enforcement action and its adequate resourcing**. In line with the establishment of a working group on the protection of minors in the Digital Services Board, and to maximise its potential for cooperation and exchange of best practices, the guidelines should require Digital Services Coordinators to: (i) dedicate specific functions, roles and responsibilities to the protection of minors; (ii) provide them with adequate expertise and resources for the task; (iii) ensure they effectively liaise with counterparts; and (iv) ensure that they are an effective and inclusive contact point for children, other citizens or civil society organisations to engage with the authority on the protection of minors, as well as for companies to be advised on compliance.

Implemented and enforced robustly, the DSA can inform the development of technology that protects and empowers children. With an outcome-based and child-rights approach, the guidelines can set a high bar for companies to comply, as well as the flexibility to innovate and invest in respecting and promoting children’s rights in the design of their services.

Signatories:

Organisations

1. 5Rights Foundation
2. A Little Lining Comes (Germany)
3. Børns Vilkår (Denmark)
4. Bris – Barnens Rätt i Samhället (Sweden)
5. Digitalt Ansvar / Digital Accountability (Denmark)
6. CCDH – Centre for Countering Digital Hate
7. Center for Missing and Exploited Children (Serbia)
8. COFACE Families Europe
9. Deutsches Kinderhilfswerk e.V. (Germany)
10. ECPAT International
11. ECPAT Hungary-Hintalovon Foundation (Hungary)
12. Eurochild
13. FICE (Croatia)
14. Instituto de Apoio à Criança (Portugal)
15. Mental Health Europe
16. Missing Children Europe
17. MyData (Global)
18. Novi put (Bosnia and Herzegovina)
19. Pancyprian Coordinating Committee for the Protection and Welfare of Children (Cyprus)
20. Pomoc Deci (Serbia)
21. Prins Carl Philips och Prinsessan Sofias Stiftelse (Sweden)
22. Red Barnet – Save The Children (Denmark)
23. Telefono Azzurro (Italy)
24. Terre des Hommes Netherlands
25. The Smile of the Child (Greece)
26. Thorn

Individual experts

27. Professor Simone van der Hof, Professor of Law and Digital technologies, Leiden University; member of the special group on an EU Code of conduct on age-appropriate design
28. Professor Anne Mette Thorhauge, Center for Tracking and Society at University of Copenhagen, member of the special group on an EU Code of conduct on age-appropriate design
29. Ingrida Milkaite, Ghent Univeristy, member of the special group on an EU Code of conduct on age-appropriate design
30. Jutta Croll, Chairwoman of Stiftung Digitale Chancen, member of the special group on an EU Code of conduct on age-appropriate design
31. Professor Dr. Konstantinos Karachalios, Former Managing Director, IEEE Standards Association
32. Mie Oehlenschläger, Co-Founder of Tech&Childhood
33. Katrine K Pedersen, Co-founder of Tech&Childhood
34. Heidi Als Ringheim, Chair of Mediahealth for Children and Youth

RESOURCES

5Rights Foundation, Eurochild and European Parliament Intergroup on Child Rights (2024), *A High Level of Privacy, Safety & Security for Minors – A best practices baseline for the implementation of the Digital Services Act for children*, available at <https://5rightsfoundation.com/resource/5rights-launches-tool-to-support-dsa-enforcement-for-children/>