Eurochild
Putting children at the heart of Europe

*Eurochild*
*Avenue des Arts 7/8, 1210 Brussels*
*Legal Address: Rue de la Charité 22, 1210 Brussels*
*Tel. +32 (0)2 511 70 83 Fax +32 (0)2 511 72 98*
*info@eurochild.org - www.eurochild.org*

# Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act

Eurochild advocates for a digital environment where children's rights are upheld. The present draft 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 show a very welcomed **child rights approach**, most notably by giving careful consideration of the possible effect of the recommended safety measures on a variety of children's rights. In this sense, there are some inconsistencies shown across the guidelines, for example in mainstreaming their right to be heard across provisions and lacking considerations on the right to access information in content moderation and recommender systems. Eurochild believes that age appropriate design is crucial to recognise the evolving and complex nature of children's needs. For the approach to be fully holistic, Child Rights Impact Assessments should be included as a core recommendation, rather than a supplementary tool. A child-rights lens necessarily encompasses a **risk-based approach**. On this note, we particularly applaud the integration of the 5Cs framework and child rights assessment tools in the risk review. We hope this can also have a positive impact on the risk assessment obligations of Articles 34 and 35 for VLOPs.

We equally welcome the broad and flexible **scope of the guidelines**, clarifying Article 28 obligations on platforms which might not be targeting or allowing minors but do not put sufficient measures in place to control it. We would welcome further clarification on what types of video games would also fall under the scope of the guidelines. Clarity of scope is crucial to avoid non-compliance by platforms.

The risk-based approach is particularly visible in the section on **age assurance**, providing much needed clarity on which methods are more appropriate based on the risks the platform may pose to children. We stress the importance, as recognised in the guidelines, of its complementary nature to other safety measures. It may be that other measures based on safety- and privacy-by-design may be sufficient to provide a high level of privacy, safety and security, making age assurance unnecessary. However, we note with concern that the assessment required by the guidelines to decide on the appropriateness of age assurance is based on the platforms' own risk review, which may render an inappropriate result, especially in light of the poor quality of the first round of risk assessment reports provided by VLOPs under article 34 and 35 of the DSA. Moreover, provisions should avoid that platforms which T&C limit users to +18 but do not pose a risk to children are subject to a blanket age verification recommendation (i.e., fashion stores or marketplaces).

The focus on **system design** is a breakthrough in the context of digital policy, putting the responsibility on online platforms in line with UN General Comment No. 25. It offers cross-sector solutions to the risks children face in these platforms on the basis of high privacy- and safety-by-design. We particularly welcome the recognition of the evolving capacities of the child in the default settings section. With regard to this, the guidelines show a good first attempt to balance detail and flexibility,. However, some of this language should be reframed under a more principled approach (followed by examples) to ensure

*Eurochild*
*Avenue des Arts 7/8, 1210 Brussels*
*Legal Address: Rue de la Charité 22, 1210 Brussels*
*Tel. +32 (0)2 511 70 83 Fax +32 (0)2 511 72 98*
*info@eurochild.org - www.eurochild.org*

the provisions remain technologically neutral and future-proof. We provide some concrete suggestions on this further below.

We would suggest **more concrete recommendations or examples on provisions related to persuasive and addictive design** in section 6.4 (account settings) and 6.6 (commercial practices). After many attempts to regulate dark patterns and deceptive practices online (i.e. art 25 DSA, art 6 - 9 of the Unfair Commercial Practices), dark patterns continue to shape children's lives online, in many cases maximising the retrieval of their data or their engagement, with negative effects on their privacy and wellbeing.

Regarding **recommender systems,** we welcome the prioritisation of 'explicit user-provided signals' over 'implicit engagement-based signals' to determine the content displayed and recommended to minors. However, when considering the objectives of the guidelines the former option should be turned on by default for children. Similarly, the parameters and evaluation strategies of recommender systems should prioritise the best interests of the child over the maximisation of engagement. To ensure that children are not exposed to illegal or harmful content by recommender systems, guidelines should also go further than the current provisions, recommending the use of content categories covering not only illegal but also harmful content, including if seen repeatedly, as a factor to shape recommended content. It is crucial that this content categorisation is done involving independent experts, civil society and children themselves.

We applaud the many **provisions targeted at empowering children** to make their own, informed decisions about their online lives, including regarding time management, default settings and recommender systems adjustments and tools for caregivers and guardians. However, one could argue that time management and default setting changes are not necessarily measures targeting interface design, as they focus on user behaviour. Therefore, we would suggest moving these measures to section 6.5 on user control and empowerment. We also recommend strengthening the provisions of child participation and make it a general principle of the guidelines.

The right of children to be protected from economic exploitation goes beyond advertisement quality and transparency. Therefore, the current provisions of the guidelines on **commercial practices** are a good starting point, but need to be complemented with other provisions related to advertisement positioning and quantity, influencer marketing, childfluencing and other manipulative practices that qualify as economic exploitation. It is the responsibility of platforms, not only creators, to ensure that children are not exposed to harmful advertisement or a quantity of advertisement that can be harmful to their wellbeing. Similarly, they should ensure that no advertisement is positioned next to harmful content, as it is often the case that advertisement might exacerbate the harm of particular pieces of content such as eating-disorder related content. Platforms should not allow any form of economic exploitation of children in their platforms, including by influencers who are allowed to monetise content portraying children, i.e., sharenting.

Additionally, we welcome the consideration of practices that can lead to excessive or unwanted spending or addictive behaviours, as well as manipulative design techniques. However, those provisions should be expanded to provide specific practices as benchmarks, such as micro-transactions, selective disclosure

*Eurochild*
*Avenue des Arts 7/8, 1210 Brussels*
*Legal Address: Rue de la Charité 22, 1210 Brussels*
*Tel. +32 (0)2 511 70 83 Fax +32 (0)2 511 72 98*
*info@eurochild.org - www.eurochild.org*

information, false hierarchies, or scarcity. The guidelines should also have stronger provisions regarding data protection and minimisation, to avoid abusive data practices for the commercial gain of platforms.

Regarding **content moderation**, we welcome the call for a clear and transparent definition of harmful content to children's privacy, safety and security, which should be defined with the involvement of not only experts and civil society but also children. Platforms' moderation procedures and policies should also be strengthened, by including an appropriate timeframe for the action upon harmful content for children, which could be established between 24 and 48 hours, and by prioritising content that may exploit children's vulnerabilities (i.e., content that may be more harmful for some children due to gender, disabilities, etc.). The guidelines should also include more targeted measures to improve content moderation on the platforms' services, such as functions that allow users to 'block' or 'hide' comments, accounts or keywords, that prevent users from bypassing a block or warning for prohibited content, etc.

Provisions on **reporting mechanisms** should highlight existing good practice to fight grooming, cyberbullying and strengthen the link with support systems and safety resources.

Similarly, we find the provisions on **Artificial Intelligence** welcome, but slightly superficial. While some AI features can be used as support measures, especially chatbots, a significant part of AI features on online platforms have a broader use. AI chatbots, for instance, have become a search engine, a creation tool, among other things, and are in many cases embedded within the experience within the platform itself. Therefore, distinct safeguards should be considered for AI chatbots, generative AI and AI as a safety tool.

When considering **AI chatbots**, guidelines must include provisions to ensure not only transparency on the interaction with a machine, but on data use, preferably encouraging children not to share sensitive or personal information. Children should not only know that they are interacting with AI, but be able to make an informed decision as to whether they want to interact with such AI. Therefore, they should not be prominently pushed or recommended to children and should be easy to turn off or disengage from their experience. Finally, they should not encourage children towards commercial content or purchases, amplify fake news and limit their ability to emulate child-like features or interactions. Regarding **generative AI**, platforms should also provide age-appropriate information about the purpose, functioning and data management of the AI system. Any AI embedded in the system that is accessible to children should be developed, trained and used ethically, considering the full spectrum of children's rights, and should provide strong safeguards to protect children from harmful content and contact, especially exploitation and abuse. Lastly, the guidelines should also consider **AI as a safety tool** and call platforms to innovate and foster the development of AI technologies designed to promote the safety of children.

Finally, the guidelines should provide more clarity on **enforcement** mechanisms, including a stricter deadline for review and recommendations to support the work of Digital Services Coordinators at national level.

For further information, please contact Fabiola Bas Palomares, Lead Policy & Advocacy Officer on Online Safety.