Eurochild contribution on recurrent and prominent systemic risks in the EU and on measures for their mitigation

Policy Paper

Eurochild
Putting children at the heart of Europe

November 2025

Eurochild contribution on recurrent and prominent systemic risks in the EU and on measures for their mitigation

This policy briefing includes Eurochild's contribution to the Board for Digital Services, following the European Commission's invitation to provide input for the preparation of the Article 35(2) DSA annual report on the most prominent systemic risks and their mitigation measures. Eurochild's contribution has not been made publicly available through the Commission's 'Have Your Say' portal.

Organisation details

Eurochild is the largest network of organisations and individuals working with and for children in Europe. With 224 members in 42 countries, we strive for a society where all children and young people grow up happy, healthy, confident and respected as individuals in their own right. We aim to put children's rights at the core of policy-making in Europe to bring positive changes to the lives of children, in particular those affected by poverty and disadvantage.

Eurochild is working together with the EU and other civil society organisations to realise children's rights both offline and online. Working across different files, we advocate for a child-centred approach in digital legislation that accounts for the rights of children and their specific needs and vulnerabilities.

This submission provides a compilation of some of the most prominent risks that children face online gathered from our experience and works with members and children, and does not aim to provide an exhaustive analysis. It focuses on those risks which are insufficiently identified by VLOPs and VLOSEs in their risk assessment reports. Given the substantial shortcomings of these reports, we call for the use of child rights impact assessments as basis for the next iteration of reports.

Question 1

The report to be published once a year by the European Board for Digital Services in cooperation with the Commission pursuant to Article 35(2) DSA should outline the most recurring and prominent risks stemming from VLOPs and VLOPSEs.

A. Please provide any information you have that is suitable for identifying and assessing systemic risks you find potentially prominent or recurrent. The submission can consistent e.g. of studies (conducted by yourself or third parties), samples of typical constellations occurring at the use of the service and relevant findings or conclusions in regards of (typical) practical experiences made by users you represent or are aware of.

To begin with, we can build on our own experience and research working directly with children and with child rights organisations across Europe. Every year, we publish the Eurochild Flagship Report providing an overview of the state of children's rights across Europe through our member input - 57 organisations covering 31 European countries in 2024. Their insights on children's rights in the digital environment are compiled in the sub-report 'Bridging persistent gaps in children's rights online in Europe'.

Consistently across all regions in Europe, the key risks identified by our members include online **child sexual abuse and exploitation** and **cyberbullying** and online harassment. While these are not new threats, they remain persistent and deeply concerning. Members also highlight emerging risks and regulatory gaps around the commercial exploitation of childfluencers, gambling-like features in videogames and age assurance. Additionally, our members report that children are accessing the internet at **increasingly younger ages**, broadening their exposure to these risks and heightening their potential impact. This issue is not properly addressed in most of the VLOPS and VLOSEs risk assessment reports, with very limited age assurance commitments and information being provided.

Alongside research with our members, we conduct direct studies with children. In 2023-2024, we consulted almost 500 children and over 6,000 caregivers across 15 countries (10 EU member states and 5 in Asia and Latin America) through the VOICE Project, aiming at better understanding their experiences and needs online.

In this study, children identified **negative mental health outcomes** as a major risk online, particularly isolation, anxiety and addiction, strongly linked to exposure to **harmful content** and **addictive digital design**. While they may not always articulate it explicitly as addiction, children in the study clearly recognized difficulties to spend less time online. Substantial evidence shows this is likely to be linked to the use of hyper-personalisation and **engagement-driven features like infinite scrolling**.

Echoing the findings from our members' report, **cyberbullying** and **online child sexual abuse** were frequently mentioned, especially in the context of how their personal information could be misused by others to harm them. This also raised concerns around **data protection and privacy.** The right to privacy of children is not adequately addressed in the VLOPs & VLOSEs risk assessments, with superficial references to high-privacy by default settings.

Combining these insights with the methodology of the 4Cs of online risks for children[1], we note that the prevalence or manifestation of certain risks vary across different types of platforms:

a. Search engine: a key concern is the high risk of children encountering misleading, harmful content or illegal content. Early exposure to such content is proven to be highly detrimental. For instance, research shows that 70% of surveyed offenders were exposed to CSAM before

[1] Livingstone, S., & Stoilova, M. (2021). The 4Cs: Classifying Online Risk to Children. (CO:RE Short Report Series on Key Topics). Hamburg: Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI); CO:RE - Children Online: Research and Evidence.

turning 18 years old, and nearly 40% before being 13[2]. Moreover, repeated exposure to harmful content (i.e., dieting or eating-disorder related content) from early ages has notable negative effects on the development of children. Currently, we note that harmful content is easily accessible and age-restrictions and content controls are easily by passable.

b. Online marketplaces: Children are rarely recognized as consumers in online marketplaces, yet in the digital environment, they actively engage in consumption—both by purchasing goods (i.e., on videogames) and consuming content in exchange of data. This constitutes a form of contractual engagement, which terms are not fairly communicated to children and are often abusive. Children frequently experience **commercial exploitation**, particularly through dark patterns that manipulate their behaviour to encourage excessive spending or use. They also face **misleading marketing**, which adults may recognize but children often do not, especially coming from influencers.

c**.** Social media: Social media platforms pose a multi-faceted range of risks. **Harmful content exposure** is fuelled by algorithmic systems trained to promote content that may be damaging to children's mental well-being and a failure to consistently remove harmful content. Social Media platforms are designed to maximize engagement, creating **addictive design patterns** that extend beyond commonly discussed elements like infinite scrolling and autoplay and signal a wider design problem. Other significant factors include popularity metrics, along with activity and push notifications, random reward mechanisms, and parasocial relationships with influencers. Children increasingly report that these platforms are difficult to disengage from - cancelling services, deleting data, or adjusting privacy settings is often too complex, making continued use the default option. This friction is intentionally designed to maximize engagement. The nature of social media leads to a high prevalence of **contact risks to children** such as grooming, online child sexual abuse, cyberbullying, harassment, and targeted hate speech. Despite their significance, addictive design, contact and privacy risks are not adequately reflected in Articles 34, 35, or other sections related to risk assessment, and therefore are insufficiently addressed in the VLOPs & VLOSEs reports.
All these risks contribute significantly to **negative mental health impacts**. Children develop extensive online networks and feel that going offline means exclusion, fostering a fear of missing out (FOMO) and disconnection from their social circles. This affects their self-esteem, social integration, and long-term development. For instance, Instagram and TikTok do not adequately address the mental health risks to children posed by features like image and video filters, which can affect seriously self-esteem and body image. Addressing online risks requires a deeper examination of the specific design mechanisms driving it.
As mentioned regarding marketing places, concerns also arise from the **risk of harmful products being sold to children by influencers and of hidden advertising**[3], which is not

[2] Redirection Survey, CSAM Users in the Dark Web: Protecting Children Through Prevention, 2021, Tegan Insoll, Anna Ovaska & Nina Vaaranen-Valkonen: p.15 and following of the report.

[3] BEUC (The European Consumer Organisation). "Children protection online in the EU" February 2025.
BEUC (The European Consumer Organisation). "Food marketing to children needs rules with teeth" July 2021 (*ante DSA adoption)*.

addressed by the online platforms likely to be most affected by this issue (Instagram, TikTok, YouTube…[4]), although some mitigation measures exist and could be adopted (e.g. age rating of videos advertising harmful content).

d. Gaming platforms: Same as social media platforms, video game companies are competing to maintain their users engaged for as long as possible to maximize their financial revenue. For this, game developers purposely embed addictive or manipulative features within the design of the games or platforms, in what is often referred to as "persuasive design", and deploy "dark patterns" that lead children to harmful behaviours. These include micro-transactions that push children to spend more on a game than intended, gambling-style features such as loot-boxes, activity- or time-based rewards that encourage children to spend more time than intended, non-transparent in-game currencies and lack of content moderation to fight hate speech, cyberbullying and child sexual abuse (especially grooming).

e. Online pornographic platforms: These platforms contribute to the **early sexualisation of children and reinforce harmful stereotypes that normalize abusive or deviant sexual behaviors**. Exposure to such content at a young age can shape distorted perceptions of relationships and consent, increasing the risk of exploitation and perpetuating harmful behaviors.

Our own internal assessment of the first round of VLOPs risk assessment reports, focused on the most prominent VLOPs hosting children and/or content potentially harmful to them (Facebook, Instagram, YouTube, TikTok, X and Snapchat), shows several inconsistencies in evaluating the risks outlined before. While cyberbullying and OCSEA are extensively addressed, little information is provided about the persistence or scale of the risks nor the efficacy of the mitigation measures. Despite the requirements of Article 34 of the DSA, there is **little emphasis on key aspects (often understood as cross-cutting risks) such as children's privacy or design choices –** particularly addictive features or dark patterns. Moreover, the **assessments often fail to identify specific gaps or emerging trends** that pose risks to children's rights online, such as Artificial Intelligence**,** indicating limited adaptability and proactivity.

More worryingly, they also **fail to address the specific risks encountered by vulnerable children, such as children with disabilities, outside of family care or from disadvantaged backgrounds.** Lastly, the assessment of the risks for children tends to focus on the characteristics of particularities of each service, rather than being grounded in children's rights or their lived experiences, which may lead to overlooking certain risks beyond those linked to the intended use of the services.

BMC Public Health. Naderer, B., Wakolbinger, M., Haider, S. *et al.* "Influencing children: food cues in YouTube content from child and youth influencers". 2024.

[4] Trekels, J., & Eggermont, S. "I Can See How Many Watched It: A Focus Group Study on Social Norms and Adolescents' YouTube Use" January 2021.

B. Where available, please include information about what makes the risk prominent or recurrent.

One of the main factors that expose children to increased risks on online platforms is the presence of **pre-existing vulnerabilities**. Adverse childhood experiences, both online and offline, can heighten their exposure to these risks. Children with disabilities represent a particularly vulnerable group, and their needs must be considered by online platforms when designing their services. Children growing outside of family care or with parents who cannot engage in parental supervision may not benefit from online protections that rely on parental controls or age assurance.

Other significant factors likely to increase risk exposure include the design of the platforms, the functioning of recommender systems, and the use of generative AI (see question 3).

C. Please specify whether the information you provide relates to a single Member State, to several Member States or whether it applies to the entire Union.

Unfortunately, in our VOICE research with children and caregivers, we were unable to conduct an in-depth geographic comparative analysis. However, when compiling results from different countries, we observed that **children across regions face similar risks.** While these risks manifest in comparable ways across regions, the underlying drivers of harm and reporting behaviors differ significantly. Across the board, we note that **children rarely use reporting mechanisms** due to a lack of trust in their effectiveness and their lack of age-appropriate language.

Even when systemic risks are the same, their impact on a child's development and their resilience to deal with those effects vary depending on cultural factors. In some societies, cultural taboos and paternalistic attitudes shape children's experiences, whereas in others, a stronger emphasis on children's rights fosters greater autonomy and agency as independent users. **Despite these variations, global trends in systemic risks remain evident.**

D. *Please refer to any existing documentation, research or resources that could help substantiate the evidence you provide.*

Referenced throughout question 1(A).

Question 2

The report to be published once a year by the European Board of Digital Services in cooperation with the Commission pursuant to Article 35(2) DSA should indicate best practices for mitigation measures implemented by the providers of VLOPs and VLOSEs.

A. Please provide examples of practices addressing any systemic risks you have identified, specifying to which systemic risks such measures relate.

While we are not in a position to endorse specific practices over others, particularly when we lack the data to assess their effectiveness in mitigating specific risks, we can assess the

overall approach of VLOPs regarding their mitigation measures, and provide for some general good practice. The mitigation measures provided in the reports are insufficient - rather than setting a higher standard for child protection, they primarily consist of longstanding safety measures without meaningful advancements.

Overall, there is a **clear lack of innovation and ambition in the mitigation measures designed for children**. Most rely on the basic prescriptions of the DSA, primarily focusing on ***content*** moderation—an approach that has existed for over 15 years. Similarly, platforms frequently cite reporting mechanisms and trusted flaggers as key mitigation tools, despite their limitations in effectively removing content, particularly 'grey content'—material that, while not explicitly illegal or in violation of terms and conditions, remains harmful to children (especially under repeated exposure). Some practices could be put forward as good practices (non-exhaustive):

- Ensure due enforcement of the platform's terms and conditions, including by committing the necessary resources to ensure effective content moderation tools and human moderation teams;
- Identify and restrict the access and recommendation to children of content that, shown repeatedly to children, can have a negative impact on their wellbeing (i.e., Meta limits the potential shares and comments on sensitive content);
- Reduce the hyper-personalisation capacity of the recommender systems and content algorithms deployed to children;
- Default content restrictions to minimize exposure to harmful content (i.e., SafeSearch by Google) and provide tools for children to curate the type of content they can access or is recommended to them, including by using content filters, tags, etc. (i.e., Keyword filters and resetting functions for FYF provided by TikTok);
- Provide tools for effective and age-appropriate reporting and redress;

Many mitigation measures centre on privacy safeguards for users under 18, such as restricting ***contact*** between minors and adults or limiting the virality of their content to reduce exposure (i.e., Meta's privacy-by-default for <18 or TikTok's restrictions on live-streaming for children). However, **the two most commonly proposed safeguards—parental controls and age verification—are often described generically**, without tailoring them to the specific risks of each platform. Their effectiveness in mitigating harm remains questionable, and they lack the necessary innovation to address emerging threats. This is specifically true for the risk of online grooming, as safeguards in private communications are rarely addressed (i.e., Snap report does not even cover private communications at all). Some good practices are (non-exhaustive):

- Ensure *comprehensive* settings are "high privacy" by default for child users (visibility of accounts, interaction with unknown accounts, limited chat functions, comments, livestreaming and shareability of the content, etc.);

- Have clear processes for modifying them according to their evolving capacities, providing the child with appropriate information;
- Deploy tools in private communications that allow children to control what type of content they receive, i.e., sensitive content controls;
- Engage in proactive detection of illegal material, especially child sexual abuse, and of suspicious accounts that contact children for harmful or illegal purposes;
- Ensure parental tools provided respect the privacy and agency of the child.

Likewise, ***conduct*** risks, most notably cyberbullying, are unevenly addressed in the reports, with only few platforms highlighting comprehensive safeguards such as Meta's content tagging controls, hidden words and comments restrictions – which should become default settings for children.

As outlined before, ***contract*** risks to children are not sufficiently addressed in the VLOPs and VLOSEs reports. The commercial exploitation of children online come from several sources. First, safeguards to protect children who are childfluencers from economic exploitation and prevent abusive data practices for child users should go beyond the banning of targeted advertisement. For instance:

- Minimise the collection and exploitation of children's data and prioritise the best interests of the child in the use of such data (i.e., YouTube's restricted data collection on content labelled as 'Made for kids');
- Provide clear and child-friendly information to children who become childfluencers and monitor parental involvement on the transactions between the child and the platform;
- Age-restrict content where an influencer advertises products that are harmful to children;
- Avoiding the placement of advertisement next to content potentially harmful to children;
- Age rating of content, especially in gaming platforms, that is based on the 4Cs of online risks, instead of just how graphic, nude or violent the content portrayed is.

Second, risks arising from specific ***design*** **architecture of platforms** are not adequately addressed in the VLOPs and VLOSEs reports. In some cases it is acknowledged as a residual risk and do recognise features such as turning off autoplay by default. In others is vaguely mentioned in the context of mental health and digital wellbeing, where platforms argue that time reminders and 'winding down' nudges sufficiently address these risks. However, these mitigation measures place the burden on the user rather than address the source of the issue within the design of the service. Some safety-by-design practices could be put forward as good practices (non-exhaustive):

- Carrying out child rights impact assessments for digital designs and online safety features targeted at children;

- Turn off profiling options by default, especially for the purpose of targeted advertisement;
- Avoid functions designed to maximise engagement, extended use or that make it difficult to turn off or exit the online experience (i.e., infinite scrolling, auto-play – as already included in YT Kids, excessive notifications, time-based rewards, nudging, etc.);
- Rely on children and child rights experts for roles and responsibilities dedicated to the protection of minors.

We have observed some platforms advancing in the provision of **child-friendly information**, especially in reporting tools and terms and conditions, which we view as a positive step in the right direction. Similarly, more and more platforms are setting up youth and children's councils to **inform their actions with children's views**. However:

- Information should not only be presented in a way that is age appropriate but also reiterated along the user journey (i.e. when specific settings are changed or gets older);
- Ensure children's views are properly integrated in the platform's design and management decisions.

B. Please refer to any existing documentation, research or resources that could help substantiate the information on the risk mitigation practices you refer to.

- Eurochild position paper on children's rights online. You can find more detail on these practices put in context of the DSA obligations on 5Rights Foundation report 'A High level of privacy, safety & security for minors'.
- CEN CENELEC Workshop Agreement on age-appropriate design.

Question 3

When conducting risk assessments, according to Article 34 (2) DSA, providers of VLOPs and VLOSEs must take into account how the identified systemic risks are influenced by* risk factors*, such as* recommender systems *and other* algorithmic systems*,* advertising *systems, and* content moderation *systems. The assessment must consider how the risks are influenced by* intentional manipulation *of the service, including by inauthentic use or* exploitation *as well as the* amplification *and potentially rapid and wide dissemination of illegal content and of information that is incompatible with their terms and conditions. The assessment shall take into account specific regional or linguistic aspects, including when specific to a Member State.

A. Please provide any information you have of the influence of these risk factors on the systemic risks you have identified.

Greater nuance is needed in understanding how algorithmic systems contribute to systemic risks. Growing evidence[5] suggests that algorithmic systems often feed harmful content to children, as they prioritize engagement, frequently driven by violent content, extreme speech, and other problematic material. As acknowledged by some platforms in their risk assessment reports[6], perpetrators of online child sexual abuse continue to circumvent content moderation tools and share CSAM openly in their platforms – special attention must be paid to how algorithmic systems may disseminate CSAM. **A key distinction must be made between merely recommending certain content and repeatedly exposing users to it. This latter aspect should be considered and exacerbating factor**.

Research shows[7] that **advertisements can still be placed next to harmful or sensitive content on online platforms**, demonstrating both the failure to remove this type of content and the possibility that online platforms may be profiting from it. This influencing factor is rarely assessed in the risk assessment reports, which in most cases only refer to the prohibition of advertising targeted at minors.

Regarding **content moderation, many platforms fail to effectively enforce age restrictions**. Even when content is labelled as age-inappropriate and subject to age-gating—meaning it should not appear in feeds of users under a certain age—enforcement remains inconsistent across platforms and individual users. Additionally, **flagged content that is deemed age-inappropriate is often not removed as expected**[8]. The risk extends beyond the content itself to the surrounding features of content moderation and algorithmic amplification, such as tagging functions, ad placement near sensitive content, and whether comments are allowed on videos featuring children. A more comprehensive approach is needed to address these risks.

Another influencing factor, identified by some VLOPs in their reports, is **Artificial Intelligence, especially content generators**. Despite still an evolving field, the generation of harmful material with AI-powered technologies is an increasing trend. This is especially dangerous when used for child sexual abuse, including grooming sexual extortion and the creation of **AI-generated CSAM** – through not only fine-tuned models but also general-purpose AI systems. Two additional concerning trends have emerged: (1) **AI-generated results reinforcing harmful stereotypes, disproportionately affecting vulnerable children**; and (2) t**he emotional manipulation of children through AI chatbots and companions**.

[5] NPR. "TikTok's Redacted Documents in Teen Safety Lawsuit Revealed" NPR, October 11, 2024.
EKO. "Suicide, Incels, and Drugs: How TikTok's deadly algorithm harms kids", March 2023.
Amnesty International. "TikTok Risks Pushing Children Towards Harmful Content" November 2023.
Center for Countering Digital Hate. "Deadly by Design" CCDH, December 2022.
Center for Countering Digital Hate. "YouTube Pushes Harmful Eating Disorder Content to Teens in EU" February 2025.
[6] Cf. Facebook risk assessment report, p.69, and Instagram risk assessment report, p.67.
[7] Center for Countering Digital Hate. "YouTube Pushes Harmful Eating Disorder Content to Teens in EU" February 2025.
[8] Center for Countering Digital Hate. "YouTube Pushes Harmful Eating Disorder Content to Teens in EU." February 2025.

Question 4

Do you have any other information and/or material relating to the Digital Services Act that you would like to share with the European Board of Digital Services and the Commission? If so, please use the reply to this question to convey it.

As already referred to in question 1, our own internal analysis of VLOPs risk assessment reports indicates a **lack of a common methodology for risk assessment** and a **fundamental shortage of data** to determine whether the identified risks are as significant as platforms suggest. This makes it difficult to assess whether their risk identification processes are adequate as well as the effectiveness of mitigation measures.

Additionally, the **absence of a standardized approach prevents meaningful comparisons** across reports (both across platforms and across years). Most assessments rely on the predefined systemic risks outlined in the DSA or the specific characteristics of individual services rather than the real experiences of children, resulting in overly theoretical evaluations that lack complexity. As a result, **cross-cutting risks are often overlooked, and emerging risks are rarely addressed**. **A standardized framework is essential to ensure a cohesive approach across platforms**. Without it, reports remain fragmented and incomplete, leaving critical gaps in understanding and mitigating risks.

There is plenty of good practice and tools that could inspire a recommended methodology for VLOPs and VLOSEs risk assessment and mitigation reports – to ensure a holistic approach to children's rights, we strongly recommend the adoption of Child Rights Impact Assessments (CRIAs) and the Livingstone & Stoilova's 4Cs classification of risk for the next round of reporting. There is extensive guidance on CRIAs[9]: the UN Convention on the Rights of the Child, UN General Comment No. 25, and UNICEF's guidance on child rights impact assessments online provide key basis for impact assessment frameworks. Additionally, the CEN CENELEC has established a workshop agreement on age-appropriate design for children, offering recommendations on risk assessment and mitigation.

A critical component needed to implement these **is improved data collection, disclosure and transparency**. Risk assessments must incorporate structured data to accurately measure the prevalence of risks and evaluate the effectiveness of mitigation measures. Additionally, platforms should actively **gather user feedback** on these measures, assessing effectiveness and uptake. This process should include qualitative insights from children, and child rights experts to also account for any unintended consequences on children's rights.

To improve accountability, **reports should integrate consistently in the risk analysis key performance metrics**, even if already provided in their Transparency Reports, such as (non-exhaustive):

[9] In addition: 'Child Rights Impact Assessment in relation to the digital environment' by BSR; & 'Child Rights Impact Assessment and Manual' developed by the Dutch Ministry for Interior

- Uptake of parental tools, wellbeing features, content controls features, reporting mechanisms, etc.
- Number of reports per content categories and age categories, allowing for an accurate evaluation of risk prevalence.
- Quality of reports: proportion of flagged content is confirmed as problematic and/or has led to law enforcement actions; proportion of illegal content identified and removed within a given timeframe (for example, before X number of views).
- Sensitive/flagged/age-restricted content recommended to children and **frequency of content shown to children**, and how recommendations vary across different user groups.

Finally, **risk assessment reports are often outdated by the time they are published and cover different time frames across platforms**. The reports released in 2025, for instance, cover the period between 2020 and 2023, failing to capture emerging trends and the associated risks.

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

For more information, contact:
Francesca Pisanu
EU Advocacy Officer, Eurochild
Francesca.pisanu@eurochild.org