Joint submission: The recurrent and prominent systemic risks faced by children and measures for their mitigation

INTRODUCTION

Together with four child rights and family organisations, we prepared this joint submission to highlight the risks faced by children in the digital environment as systemic and recurrent. The following contribution focuses on actual or foreseeable negative effects on the exercise of children's rights, emphasising that many of those risks are still under-identified and under-analysed by VLOPs and VLOSEs. Risks are directly linked to the design choices of platforms; however, many of VLOPs and VLOSEs fail to recognise those crucial risk factors. We therefore strongly recommend the use of child rights impact assessment as a tool to ensure the proper identification of risks, the recognition of design choices as risk factors and a detailed and evidenced-based assessment of mitigation measures.

We would like to note that this submission does not represent a comprehensive and holistic evaluation of all the risk assessments of the VLOPs and VLOSEs but rather a snapshot analysis, presenting some key trends and providing some insights for improvements.

1. IDENTIFYING AND ASSESSING SYSTEMIC RISKS

Under article 34(1) of the DSA, systemic risks include (a) the dissemination of illegal content through their services, (b) any actual or foreseeable negative effects for the exercise of fundamental rights, in particular respect to the rights of the child, (d) any actual or foreseeable negative effects in relation to gender-based violence, the protection of public health and minors and serious negative consequences to the person's physical and mental well-being.

To identify and assess systemic risks in relation to child rights, tools such a Child Rights Impact Assessments (CRIA) should be used by companies. A CRIA can be considered as a specific form of a Human Rights Impact Assessment.[1] It is an instrument to assess the impact of a policy, proposed legislation, administrative measures or budgetary allocation on children. Increasingly, they have been recognised as a tool to help companies ask the right questions, notably in the digital environment.[2] UN General Comment No.25 on children's rights in relation to the digital environment specifically mentions CRIA as a requirement that should be imposed on the business sector.[3] This tool enables the identification of both positive and negative impacts on all children's rights. It provides for a holistic and systemic approach, encompassing the full scope of the UN Convention on the Rights of the Child, from the right to participation, right to health and development, access to reliable information, protection from commercial exploitation and protection from sexual exploitation, as well as

[1] Digital Futures Commission (2021) Child Rights Impact Assessment: a tool to realise children's rights in the digital environment.
[2] See Digital Futures Commission (2021) Child Rights Impact Assessment: a tool to realise children's rights in the digital environment.
[3] Committee on the Rights of the Child (2021) General comment No.25 on children's rights in relation to the digital environment, §23 and 38.

privacy.[4] A CRIA therefore enables the identification of all the systemic risks mentioned in article 34 that are relevant to children.

The assessment should pay special attention to the differentiated impact on children.[5] Children can have different experiences based on their age, gender identity, sexual orientation, migration status, disability status, family type or any other circumstance or condition.[6] The rights of all children should be protected and promoted.

Existing guidance on CRIAs:

- BSR (2025) Child Rights Impact Assessment in relation to the digital environment
- Dutch Ministry of the Interior and Kingdom Relations (BZK) Child Rights Impact Assessment and Manual
- UNICEF (2019) MO-CRIA: Child Rights Impact Self-Assessment Tool for Mobile Operators

Additional guidance on conducting impact assessment in relation to children and the digital environment:

- Information Commissioner's Office (2023) Children's Code Self-Assessment Risk Tool
- CEN-CENELEC (2023) Workshop Agreement for Age Appropriate Design of Services

The CEN-CENELEC Workshop Agreement: Age appropriate digital services framework sets out a process and criteria for organisations to undertake Child Rights Impact Assessments, providing an authoritative minimum standard against which the DSA CRIA should be judged.

CEN-CENELEC Workshop Agreement: Age appropriate digital services framework

> 7.3 Activities and tasks
>
> The project shall implement the following activities and tasks in accordance with applicable organization policies and procedures with respect to the child rights impact assessment as follows:
>
> **a) Undertake an initial impact assessment of how your product or service upholds children's rights, and promotes their well-being**

[4] See minimum requirements for a CRIA: Committee on the Rights of the Child (2013) General comment No.14 on the rights of the child to have his or her best interests taken as a primary consideration, §99.
[5] See minimum requirements for a CRIA: Committee on the Rights of the Child (2013) General comment No.14 on the rights of the child to have his or her best interests taken as a primary consideration, §99.
[6] See for LGBTQ+ experiences: Thorn (2023) LGBTQ+ Youth Perspectives: How LGBTQ+ Youth are Navigating Exploration and Risks of Sexual Exploitation Online; see for children with disabilities: CoE (2019) Two clicks forward, and one click back: Report on children with disabilities in the digital environment.

1) Organize your team and appoint role holders and verify that they act in good faith and in the best interests of the child

2) Plan for and identify key stakeholders to participate in the impact assessment through the following means:

i) Forming a representative panel of stakeholders or independent stakeholder advocates with sufficient expertise to represent all parties

ii) Creating mechanisms by which a diverse range of children can be consulted directly or with the help of a third party. This may be through participation on your stakeholders' panel or through other means. This could be interviews, focus groups, surveys, or formal participatory and codesign processes, among others.

3) Identify and record all impact on children's rights and well-being and address all the known sources of common hazards or opportunities in addition to identifying further sources of hazards that may be unique to the product or service, verifying that they include the following:

i) All functional, non-functional, and operational aspects and scenarios that potentially impact children, with due regard for the evolving capacities of the child, differences between children in terms of age and capacity, and also intersectional vulnerabilities such as gender, ethnicity, and disability

ii) Both intentional impacts and unintentional impacts on children's rights and well-being

iii) Normal and misuse/abuse cases

iv) Accounting for all risks to children, according to the OECD risk typology, including content, contract, conduct, consumer risks as well as the cross-cutting risks (privacy risks, advanced technology risks and risks to health and well- Being

NOTE: consumer risks also include contract risks

v) Accounting for any legislation or protections that pertain to your jurisdiction, including fair terms, data protection law, and human rights law

vi) Accounting for children's rights under the UNCRC, including specifically the UN General Comment 25 on children's rights in relation to the digital environment

vii) Accounting for risks arising from your data processing

viii) Accounting for risks that arise from design features deployed in combination with other features, which in isolation are not judged problematic

ix) Accounting for risks that develop over time as well as those that present immediate risk of harm

4) Consult and verify the outcomes with your stakeholders' panel or stakeholders' advocates, including children and parents

5) Verify that children's views are reflected through additional means where necessary, which may involve your diverse range of mechanisms and diverse consultation mechanisms (as required by 7.3.a.1.ii)

6) Document all impacts on children as agreed by your team and stakeholders and children

7) Identify and note all legal, regulatory, and best practice requirements for the product or service that need to be implemented.

b) Establish an Age Appropriate Register (AAR)

1) Adopt or define an appropriate information structure and platform for an AAR (see Annex B)

2) Record all hazards, opportunities, associated preliminary mitigation or fostering measures, as well as legal and best practice requirements

Consider publishing the findings of your Preparation phase and AAR

NOTE—These activities can benefit from close cooperation with stakeholders and

the guidance of the age appropriate value lead.

While conducting a CRIA, digital services providers must have a comprehensive understanding of the different risks to which children are exposed in the digital environment. Those risks have been classified under the 4Cs or 5Cs framework: contact, content, conduct, consumer risks and cross-cutting risks. This framework is set out in the OECD Typology of risks, children in the digital environment.[7]

- Content risks: illegal content, harmful content, hateful content and disinformation.
- Conduct risks: hateful behaviour, illegal behaviour, harmful behaviour and user-generated problematic behaviour; such as cyber-bullying and sexting.
- Contact risks: when children interact in the online environment and entail: i) children are exposed to hateful encounters in the digital environment; ii) the encounter takes place with the intention to harm the child; iii) the encounter is prosecutable under criminal law; and iv) the encounter is problematic but cannot be placed under the three previous risk manifestations. Examples are sextortion and cyber grooming.
- Consumer risks: i) they receive online marketing messages that are inappropriate for children (e.g. for age-restricted products such as alcohol); ii) they are exposed to commercial messages that are not readily identified as such (e.g. product placements) or that are intended only for adults (e.g. dating services); or iii) their credulity and inexperience are exploited, possibly creating an economic risk (e.g. online frauds).
- Cross-cutting risks: privacy risks (considering data given, data traces and inferred data), advanced technology risks (such as AI), health and wellbeing risks such as

[7] OECD (2021) Revised Typology of Risks, Children in the digital environment.

risks to mental health and physical health linked notably to prolonged screen time,[8] resulting notably from addictive and persuasive design features.

Conducting a CRIA would be highly beneficial considering the current piecemeal assessments from VLOPs. Many of the risk assessments indeed fail to consider risks to health, including mental and physical health for children, problematic use and behavioural addictions.[9] When asked about the aspects of social media they disliked the most, children note that : "*They can create addiction and isolate you from society. [And] there's a risk of receiving bad information.*"[10] META's assessment appears only to consider protection of minors, rather than the full breadth of children's rights.[11] While TikTok mentions the 4Cs framework, notably the content, conduct and contact risks, it fails to consider consumers and cross-cutting risks altogether.[12] None of the risk assessments systemically consider the differing experiences of children, presenting children as one homogeneous group with little consideration for their evolving capacities or other characteristics.[13]

Furthermore, some platforms assert that their services are simply not aimed at minors nor predominantly used by them without providing for the corresponding evidence. TikTok mentions that it is not specifically aimed at minors nor predominantly used by them[14] while reports and surveys systemically highlight that TikTok is one of the most used platforms by children.[15] X claims that its service is not targeted at younger users and that it estimates that 2% of its EU users were minors - representing overall a significant number of children.[16] In its audit implementation report, X justifies its non-implementation of the recommendation regarding the protection of minors based on the "small proportion of account holders" who are children.[17]

Additionally, to ensure a comprehensive assessment, VLOPs and VLOSEs must consult with children as recipients of the service, as well as independent children's rights experts and civil society organisations as is explicitly mentioned in recital 90 of the DSA. As children's rights organisations, we have not been consulted by any of the VLOPs or VLOSEs. Some of the interactions mentioned, for instance by TikTok, lack details and clarity as to how they effectively fed into their risks assessments, both in terms of assessing the risks and designing mitigation measures.[18]

---

[8] Expert Committee (2024) Enfants et écrans: à la recherche du temps perdu.
[9] DSA Civil Society Coordination Group (2025) Initial Analysis on the First Round of Risk Assessments Reports under the EU Digital Services Act, p.3.
[10] ECPAT, Eurochild, Terre des Hommes Netherlands (2024) VOICE project, Speaking up for change Children's and caregivers' voices for safer online experiences, p.27
[11] Meta (2024) Systemic Risk Assessment and Mitigation Report for Facebook, p.24.
[12] TikTok (2023) DSA Risk Assessment Report 2023, p.16.
[13] The JRC (2025) Social media usage and adolescents' mental health in the EU study highlights the need for gender sensitive and context specific interventions and policies.
[14] TikTok (2023) DSA Risk Assessment Report 2023, p.7.
[15] Eurobarometer (2023) Media & News Survey 2023; OFCOM (2024) Children and Parents: Media Use and Attitudes 2023; Pew Research Centre (2024) Teens, social media and technology 2023.
[16] Twitter International Unlimited (2023) Report setting out the results of Twitter International Unlimited Company Risk Assessment pursuant to Article 34 of the Digital Services Act, p.42.
[17] Twitter International Unlimited (2024) X Audit Implementation Report.
[18] TikTok (2023) DSA Risk Assessment Report 2023, p.18.

2. BEST PRACTICES

Existing international guidelines and best practices are numerous and provide for some additional practical details as to how to ensure the respect of children's rights online. Besides the UN General comment no.25, relevant guidelines include the Children's Code, the Swedish Stakeholder Guide, the Irish Fundamentals, the Dutch Code for Children's Right, the Danish Ethical Guidelines for Digital Service Providers and CNIL Recommendations on the Digital Rights of Children.

While the following highlights some of the good practices mentioned in VLOPs and VLOSEs risk assessment report, it must be recognised that details and information remain limited as to the effectiveness of those measures and as to their implementation. A recent report by CCDH on Youtube highlighted how crisis panels, presented as a mitigation measure as they direct users to resources such as helplines, were not implemented across the EU but only in 2 member states.[19] Some VLOPs also mention the possibility to block and report users, but do not provide further details as to how often those mechanisms are used or how useful children might find them.[20] Research actually shows the limited effectiveness and the difficulty of using such features.[21] Additionally, some of the measures are steps in the right direction, but are not necessarily representative of "best" practices yet. For instance, certain features mentioned under age appropriate design could be transformed into default settings. Finally, for some of the categories below, it was difficult to find examples of best practices underlining the lack of consideration for international guidelines on the topic by VLOPs and VLOSEs, as well as engagement with experts.

Default settings: they are changes made to the design of the service that provide default protections. Such measures include settings "high privacy" by default, turning off geolocation, microphone and camera off by default.[22] Default settings are critical to ensure a safe experience for children online and must be provided across platforms. For instance, in cases of sextortion, offenders often migrate children to platforms where they can easily access and monitor their contacts, using this information to further exploit them. Some platforms do not automatically set friends or contacts to private, leaving children vulnerable unless they manually adjust their privacy settings.

- Youtube: The autoplay setting on YouTube Kids and YouTube Supervised Experience turned off by default, take A Break and Bedtime reminders are turned "on" by default.[23]
- Youtube: On content 'Made for Kids', some features are not available such as comments and notifications.[24]
- Google: SafeSearch filtering on by default.[25]

---

[19] Center for Countering Digital Hate (2025) Youtube's EU Anoxeria Algorithm.
[20] Pinterest (2024) Digital Services Act Risk Assessment and Mitigation Report 2024,p.34; TikTok (2023) DSA Risk Assessment Report 2023, p.21.
[21] Thorn (2023) Responding to online threats: minors' perspectives on disclosing, reporting and blocking in 2021; European Women's Lobby (2024) Report on cyberviolence against women; Global Witness and Internet Freedom Foundation (2024) Letting Hate Flourish.
[22] 5Rights (2022) Approaches to Children's Data Protection, p.29.
[23] Google (2024) Report of Systemic Risk Assessments, p.108.
[24] Google (2024) Report of Systemic Risk Assessments, p.108.
[25] Google (2024) Report of Systemic Risk Assessments, p.62.

- Meta: On Facebook, private is the default mode for users under 18 in the EU/UK and for users under 16 in the rest of the world.[26]
- X: high privacy, safety and security settings are set for users who access X without logging into an account. All new users have personalisation turned off by default, direct messages defaulted as closed.[27]
- Appstore: personalised recommendations are not available for child accounts (under 13) and teen accounts (under 18). Teen account users can turn personalised recommendations on.[28]
- Pinterest: The profiles of users under the age of 16 are set to private as the default and only option, and in the EU, the accounts of users aged 16 and 17 are set to private by default with the option to switch to a public account. Teens who are 16 and 17 can only receive messages from mutual followers, and can only receive message requests from users they follow.[29]
- TikTok: under 18 accounts cannot host live–stream, the daily screen time is set to 60 minutes for younger users. For users between 13-15, accounts are defaulted to only allow Friends to comment on users' content.[30]

Privacy and online safety tools: they are changes that provide new mechanisms for users to control how certain features of the platform work, they must be user generated rather than provided by default.

- Meta: Hidden Words Function to empower users to filter out potentially offensive messages and comments on Meta's platforms.[31] Tag and Mention controls allow users to choose whether they want everyone, only people they follow, or no one to be able to tag or mention them in a comment, caption or Story. [32] It should be noted that this tag and mention control should become a default setting for children and be made age appropriate as well.
- Meta: Blocking mechanism allows users to prevent another user from seeing their activity, including their profile, posts or stories.[33] Facebook allows you to block your friends from viewing your list of friends. However, this feature does not exist on Instagram. Sexual extortion criminals use this specific feature to blackmail child users or befriend more children to continue perpetrating child abuse.[34]
- TikTok: offer tools to control who can comment on their content, filter and delete comments and to make certain choices about who can watch and interact with videos that they create.[35]

---

[26] Meta (2024) Systemic Risk Assessment and Mitigation Report for Facebook, p.50.
[27] Twitter International Unlimited (2023) Report setting out the results of Twitter International Unlimited Company Risk Assessment pursuant to Article 34 of the Digital Services Act, p.43.
[28] Apple Distribution International Limited (2024) App Store - Report on Risk Assessment and Risk Mitigation Measures, p.16.
[29] Pinterest (2024) Digital Services Act Risk Assessment and Mitigation Report 2024,p.33-34.
[30] TikTok (2023) DSA Risk Assessment Report 2023, p.21.
[31] Meta (2024) Systemic Risk Assessment and Mitigation Report for Facebook, p.49.
[32] Meta (2024) Systemic Risk Assessment and Mitigation Report for Facebook, p.50.
[33] Meta (2024) Systemic Risk Assessment and Mitigation Report for Facebook, p.47.
[34] Network Contagion Research Institute (2024) A digital pandemic: Uncovering the role of 'Yahoo Boys' in the surge of social media-enabled financial sextortion targeting minors.
[35] TikTok (2023) DSA Risk Assessment Report 2023, p.21.

Recommender systems: recommender systems shape online experiences notably by pushing content onto children and suggesting to add new friends into one's network. While some of the VLOPs present some measures in terms of adapting their recommender systems, their effectiveness still needs to be demonstrated.[36] Indeed, according to a Greek study, in the past year, 22.8% of children reported being exposed to age-inappropriate content at least once.[37]

- YouTube: limiting repeated recommendations of videos related to certain topics for teens.[38]
- Meta: limiting the role of shares and comments in the distribution of sensitive topics.[39] Meta also gives the ability to control how much of certain types of content (including sensitive or low quality content) are in one's feed.[40] It should be noted however that recent research demonstrates that functionalities to hide certain types of content do not work as promised, with more than 56% of posts on suggested for you feed labelled as unwanted.[41]
- TikTok: Tools to diversify the content displayed in FYF, including information about recommended videos, blocking certain keywords and to reset the recommendations.[42]
- X: Eligibility requirements before recommending content and accounts. Advertisements containing age-inappropriate content will be tagged as "not family safe" and will also be restricted to minors.[43]
- Pinterest: Private profiles are undiscoverable on Pinterest search and search engines.[44]

Data minimisation and sharing: under existing best practices,[45] only the minimum amount of personal data needed to provide the elements of the service in which a child is actively and knowingly engaged should be collected and retained. Children must have separate choices over which elements they wish to activate. Every form of optional use of personal data (including by third parties), including every use for the purpose of personalising the service, must be individually selected and activated by the child.[46] Overall, there seems to be limited engagement with data minimisation principles across the risks assessments.

- YouTube: data collection is restricted on content 'Made for Kids'.[47]

Age assurance tools: age assurance can be a powerful tool to keep children safe online, notably by enabling them to access age-appropriate experiences. Age assurance mechanisms must be proportionate to risk and purpose, privacy preserving, provide for a

---

[36] Digital Futures for Children (2024) Impact of regulation on children's digital lives, p.40.
[37] KMOP (2025), Stances and behaviours of children in online environments: Research results from Greece (as part of the CSAPE project).
[38] Digital Futures for Children (2024) Impact of regulation on children's digital lives, p.39.
[39] Meta (2024) Systemic Risk Assessment and Mitigation Report for Facebook, p.29.
[40] Meta (2024) Systemic Risk Assessment and Mitigation Report for Facebook, p.58.
[41] Panoptykon (2023) Prototyping User Empowerment.
[42] TikTok (2023) DSA Risk Assessment Report 2023, p.22.
[43] Twitter International Unlimited (2023) Report setting out the results of Twitter International Unlimited Company Risk Assessment pursuant to Article 34 of the Digital Services Act, p.44.
[44] Pinterest (2024) Digital Services Act Risk Assessment and Mitigation Report 2024,p.33.
[45] 5Rights (2024) A high level of privacy, safety and security, p.21.
[46] Ministry of the Interior and Kingdom Relations of the Netherlands (2021) Code for Children's Rights, Principle 3.
[47] Google (2024) Report of Systemic Risk Assessments, p.107.

high level of security, offer routes to challenges and redress and be accessible and inclusive.[48] While many of the VLOPs and VLOSEs did consider some types of age assurance mechanisms, mostly self–declaration, the existing risk assessments provide little detail and clarity as to considerations relating to privacy, redress mechanisms and overall accessibility for children.

- TikTok mentions its appeal process but does not provide details as to how it functions, whether it's child friendly and generally accessible.[49]
- Snapchat refers to the action it takes to terminate an account where it finds it belongs to someone 13, but does not detail whether there is an appeal process and whether it is accessible for children.[50]

Transparency: children must be given clear and appropriate information.[51] Services must avoid the use of misleading interfaces, nudges and dark patterns, and involve children in the design process of the interfaces they encounter.[52] Children themselves note that :"*If we are not aware [of] how to protect ourselves. This can increase the risk*."[53] Published terms must be presented in an age appropriate manner, ensuring that they are comprehensible, easy to find, introduced at the right moment and of an appropriate length.[54] Broadly, risk assessments rarely consider how their terms and conditions are being presented to children, whether their interfaces are easy for children to understand and to navigate, including in terms of setting up specific features.

Reporting, complaints and redress: children must be able to easily access reporting and redress mechanisms. Recital 89 of the DSA specifies that services must be organised in a way that allows easy access to minors for mechanisms, such as notice and action and complaint mechanisms. Making such services child-friendly is essential to enable children to use those mechanisms. A Greek study has shown that one in three children (aged 9-12) does not know how to use blocking or reporting tools online.[55] Currently reporting processes present the following key issues: delayed content removal, cumbersome reporting forms and evidence preservation after blocking.[56]

1. Delayed Content Removal: Minor victims report that content remains online even after being reported, sometimes for more than two weeks. Meta services, in particular, are frequently flagged for such delays.

---

[48] 5Rights (2021) But how do they know it is a child? Age assurance in the digital world.
[49] TikTok (2023) DSA Risk Assessment Report 2023, p.20.
[50] Snap (2024) Snap DSA Report: risk assessment results and mitigations, p.205.
[51] 5Rights (2022) Approaches to Children's Data Protection, p.30-31.
[52] CNIL (2021) Digital Rights of Children.
[53] ECPAT, Eurochild, Terre des Hommes Netherlands (2024) VOICE project, Speaking up for change Children's and caregivers' voices for safer online experiences, p.31.
[54] 5Rights (2021) Tick to Agree - Age Appropriate presentation of published terms.
[55] KMOP (2025), Stances and behaviours of children in online environments: Research results from Greece (as part of the CSAPE project).
[56] See ARCOM (2023) Combating the dissemination of hate content online: an assessment of the resources implemented by online platforms in 2022 and outlook Image; Thorn (2023) Responding to online threats: minors' perspectives on disclosing, reporting and blocking in 2021.

2. Cumbersome Reporting Forms: Some platforms, like Instagram, require users to complete lengthy questionnaires, making the reporting process less accessible and potentially discouraging victims from seeking help.

3. Evidence Preservation After Blocking: In some cases, when children block certain contacts, they lose access to past conversations, making it difficult to gather evidence. It should always be possible to retain access to these conversations, even after blocking, to support investigations and protect victims.

Overall, it appears that VLOPs and VLOSEs have paid little attention to how those mechanisms are used by children and how they could be improved - confirming previous findings.[57] Issues with reporting processes have been well-evidenced within external research and are seldom mentioned within the risk assessment, pointing to a broader lack of engagement with external actors in their preparation.

Detection tools and policy: Online platforms must provide detailed, transparent information on the methods they use to detect Child Sexual Exploitation and Abuse (CSEA) and their content moderation practices. This should encompass the scale and scope of their moderation efforts, the specific automated tools deployed, and any innovative approaches or strategies they are using. In addition, platforms should report on the trends, successes, and challenges they face in detecting CSEA, as well as the areas where they are focusing their ongoing efforts.

This level of transparency is crucial, as users—particularly children and their guardians—have the right to understand how automated tools are being used, how content is being scanned, the timeframes for content removal, and what happens to the content that is flagged. Furthermore, such transparency should act as a deterrent to potential offenders, challenging the prevailing sense of impunity by showing that robust systems are in place to identify and address CSEA. By providing this information, platforms can demonstrate their commitment to tackling these issues while giving users confidence in the effectiveness of these tools.

Research undertaken by the OECD shows that many of the policies remain limited in addressing CSEA and lack in details and clear explanation. Similarly, many of the services fail to provide comprehensive information regarding their content moderation.[58]

Parental controls tools: children should be given age-appropriate information about parental controls and provided an obvious sign when they are being monitored by a parent or carer.[59] While many digital services providers mention their parental control tools, many do not specify to which extent children are aware of the tools and whether they are provided with age appropriate information.[60] Children want to be informed and highlight that : *“Parents need to monitor what children are viewing online to ensure safety but, on the other hand, too*

[57] Digital Futures for Children (2024) Impact of regulation on children’s digital lives, p.34.
[58] OECD (2023) Transparency reporting on child sexual exploitation and abuse online.
[59] 5Rights (2022) Approaches to Children’s Data Protection, p.31-32.
[60] For instance: Google (2024) Report of Systemic Risk Assessments, p.107; Snap (2024) Snap DSA Report: risk assessment results and mitigations, p.202-205.

much monitoring from parents may make children uncomfortable".[61] Additionally, research shows that many parents do not understand how these tools work, do not always have the time to be involved, and that they can be hard to access and use.[62] If VLOPs rely on those tools as mitigation measures, they must provide for detailed assessments as to their effectiveness, consider their impact on children's rights, notably the right to privacy and non-discrimination, and involve the views of parents/caregivers and children.

3. RISK FACTORS

As specified under article 34(2) of the DSA, providers of VLOPs and VLOSEs must take into account how the identified systemic risks are influenced by risk factors: including, **recommender systems** and other **algorithmic systems**, **advertising** systems, and **content moderation** systems, applicable terms and conditions and their enforcement and data related practices. More broadly, and as mentioned in article 34(1) of the DSA, providers should analyse risks stemming **from the design** of their platforms. Under recital 81, it is further specified that risks may arise in relation to the design of online interfaces which may cause addictive behaviour.

Risks to children's rights are directly linked to the **design** of online platforms and search engines, as it has been demonstrated by numerous research. Design objectives relating to maximising time spent, reach and activity impact on children leading them to spend more time online, being contacted by strangers, feeling pressure to act in a certain way to gain attention and validation, etc.[63] To reach those objectives, digital services providers rely on design strategies such as refining content, applying time pressure, building anticipation, attaching value, quantifying, rewarding, making it easy to share and to interact. Those design strategies translate into well-known features present across platforms: push notifications, endless scrolling feeds, quantifying and displaying popularity, in-app or in-game purchase.[64]

- Google: "YouTube considered numerous risks particular to children [...] the risk that YouTube stimulates behavioural addictions in children"[65].
- X recognises the risk that user visibility engagement metrics could lead to unhealthy comparisons and anxiety and that scrolling design and long threats can encourage excessive use and cause cognitive fatigue.[66] None of the mitigation measures address the risks factors identified and the report simply states that there is a "lack of product solutions to decrease excessive usage time".[67]

---

[61] ECPAT, Eurochild, Terre des Hommes Netherlands (2024) VOICE project, Speaking up for change Children's and caregivers' voices for safer online experiences, p.51.
[62] Mindy Brooks, head of Google Kids and Families stated "Parents are spending "upwards of four to 12 hours a week trying to manage their kids online usage", Politico Pro Morning Tech Europe, 5 March 2025, link here; Ofcom (2012) Parent's views on parental controls; US Judiciary Committee (31 January 2024) Hearing: Big tech and the Online child Sexual Exploitation Crisis.
[63] 5Rights (2021) Pathways: how digital design put children at risk.
[64] 5Rights (2021) Pathways: how digital design put children at risk.
[65] Google (2024) Report of Systemic Risk Assessments, p.106.
[66] Twitter International Unlimited (2023) Report setting out the results of Twitter International Unlimited Company Risk Assessment pursuant to Article 34 of the Digital Services Act, p.43.
[67] Twitter International Unlimited (2023) Report setting out the results of Twitter International Unlimited Company Risk Assessment pursuant to Article 34 of the Digital Services Act, p.42.

- Instagram and Tiktok's report fails to consider the mental health risks posed by features such as image and video filters.

Recommender systems and other algorithmic systems: Automated pathways lead to graphic images of self-harm, extreme diets, pornography, extremist content and introduction to adult strangers, amongst others.[68] Even if the content may not be harmful in isolation, repeated and rapid exposure may prove harmful. Recommender systems have also a direct impact on children's right to access to information as they can narrow the type of information to which a child has access. Additionally, the use of different generative AI tools should be considered as a significant risk factor as it can lead to increased risks for children in terms of sexual abuse, their mental, cognitive and social development as well as for their privacy.[69] Meta and Pinterest recognise some of the potential risks linked to AI.[70]

- TikTok For You feed encourages self-harm and suicidal ideation, with its recommender system pushing videos relating to mental health struggles,[71] eating disorders and self-harm content,[72] and perpetuate negative or damaging ethnic stereotypes and negative and damaging gender stereotypes.[73]
- YouTube recommender system keeps on promoting harmful content to children. Recent research conducted by CCDH showed that 1 in 3 videos recommended to a fictional 13 years old contained eating disorder content.[74]
- Snapchat does not consider risks in relation to some of its most prominent features, notably in relation to Snapmap and to myAI. Although, both have been shown to present risks to children, notably in terms of privacy.[75]

Advertising systems: Children are prime targets of advertisements as they can have a significant influence over the purchases of the household.[76] Internal documentation from META shows evidence of plans to target 10 to 12 years old as a "valuable but untapped audience".[77] Advertising systems are related to commercial profiling which pose significant risks to children's privacy, their right to be free from commercial exploitation and their right to

---

[68] 5Rights (2021) Pathways: how digital design put children at risk.
[69] See Council of Europe (2023) Study on the impact of artificial intelligence systems, their potential for promoting equality, including gender equality, and the risks they may cause in relation to non-discrimination, Internet Watch Foundation (2023) How AI is being abused to create child sexual abuse imagery, Joint Research Centre (2022) Artificial Intelligence and the Rights of the Child: towards an Integrated agenda for research and policy, Norwegian Consumer Council (2023) Ghost in the Machine: Addressing the consumer harms of generative AI, Nina Dakota Szyf et al. (2024) Deepnudes among young people in Belgium: the numbers, the market, the impact.
[70] Meta (2024) Systemic Risk Assessment and Mitigation Report for Facebook, p.37; Pinterest (2024) Digital Services Act Risk Assessment and Mitigation Report 2024,p.5; TikTok (2023) DSA Risk Assessment Report 2023, p.8.
[71] Amnesty International (2023) Driven into the Darkness: How TikTok's 'For You' Feed encourages self-harm and ideal suicidal ideation and I Feel Exposed: caught in TikTok's global surveillance web.
[72] CCDH (2022) Deadly by design: TikTok pushes harmful content promoting eating disorders and self-harm into young users' feed.
[73] Reset Australia (2021) Surveilling young people online: An investigation into TikTok's data processing practices, p.21.
[74] Center for Countering Digital Hate (2025) Youtube's EU Anoxeria Algorithm.
[75] Borns Vilkar (2024) Borns Liv Med Sociale Medier, p.54-66.
[76] US Judiciary Committee (31 January 2024) Hearing: Big tech and the Online child Sexual Exploitation Crisis.
[77] US Judiciary Committee (31 January 2024) Hearing: Big tech and the Online child Sexual Exploitation Crisis.

freedom of expression and access to information.[78] Children are particularly vulnerable to the persuasive effects of advertising, notably because of their developing impulse-control and critical skills.[79] The DSA, in its article 28(2), contains a clear prohibition on targeted advertising for minors which appear to have been implemented by many VLOPs and VLOSEs. Some of the platforms also limit specific type of ads that can be shown to children.[80] Additionally, platforms should consider the impact of influencers, as they may promote gambling, drugs, replicate stereotypes, promote harmful products for children and influence their self-perception amongst other risks.[81]

Data practices: In general, users have a very limited understanding as to how their personal data is used, how the company collects and processes the data and what it is used for.[82] Research shows that children are worried about the amount of data being collected, and how that data is being used for recommender systems leading to risks in terms of harmful content.[83]

[78] UNICEF (2019) Children and Digital Marketing: Rights, risks and opportunities; S. van der Hof (2020) The Child's Right to Protection against Economic Exploitation in the Digital World.
[79] M. Rahali and . Livingstone (2022) #SponsoredAds: Monitoring influencer marketing to young audiences.
[80] Meta (2024) Systemic Risk Assessment and Mitigation Report for Facebook, p.47.
[81] E. Dreyfus (January 2024) Our kids are living in a different digital world, New York Times; Ope Adetayo (December 2023) Influencers are getting young Nigerians hooked on online gambling, Rest of the World; Revealing Reality (2024) Children's Media Lives 2024 Ten years of longitudinal research.
[82] US Judiciary Committee (31 January 2024) Hearing: Big tech and the Online child Sexual Exploitation Crisis.
[83] Reset Australia (2021) Surveilling young people online: An investigation into TikTok's data processing practices.

Please include a short description of your organisation's areas of activity and provide a contact point at your organisation

5Rights Foundation develops policy, creates innovative frameworks, develops technical standards, publishes research, challenges received narratives and ensure that children's rights and needs are recognised and prioritised in the digital world. While 5Rights works exclusively on behalf of and with children and young people under 18, our solutions and strategies are relevant to many other communities. Our focus is on implementable change and our work is cited and used widely around the world. We work with governments, inter-governmental institutions, professional associations, academics, businesses, and children, so that digital products and services can impact positively on the experiences of young people.

Contact point: Manon Baert, Senior EU Affairs Officer, manon@5rightsfoundation.com

ECPAT is a global network of 134 civil society organisations in 110 countries with one clear goal: to put an end to the sexual exploitation of children in all its forms, including technology facilitated and online sexual exploitation of children, sexual exploitation of boys in both online and offline environments, exploitation through prostitution, trafficking, early and forced marriage, and abuse in the context of travel and tourism. ECPAT engages in rigorous research, targeted advocacy, and capacity development with governments, NGOs, and the private sector to achieve this goal. We are confident that ending child sexual exploitation requires a comprehensive, multi-faceted approach. This approach must address the root causes of sexual exploitation while providing sustainable, child- centred, and child-led solutions. We are committed to creating a world where every child is safe, empowered, and free from sexual exploitation. This is our mission, and we will achieve it.

Contact point: Dr. Salla Huikuri, Head of Child Protection and Technologies, sallah@ecpat.org

Terre des Hommes Netherlands is an international non-governmental organisation committed to stopping child exploitation in four regions: Asia, Africa, Europe and the Middle East. Since 1965, TdH NL has protected children around the world from violence, harmful labour, trafficking, sexual exploitation, malnutrition and health issues. Our mission is to protect children by preventing and stopping child exploitation, engaging with partners to tackle the root causes of child exploitation. And by empowering children to make their voices count. TdH NL is a member of the Terre des Hommes International Federation.

Contact point: Nathalie Meurens, Senior EU Advocacy Manager, n.meurens@tdh.nl.

COFACE Families Europe is a pluralistic network with more than 50 member organisations in 25 European countries representing millions of families, volunteers, and professionals and promoting the well-being, health and security of families of all types without discrimination. Our area of work includes social and family policy, education, disability rights, gender equality, children rights, migration, consumer issues as well as the impact of technological developments on families. COFACE uses a multigenerational approach based on the interrelated well-being of children and their families.

ch
Contact point: Beatrijs Gelders, Policy and Advocacy Officer on Safer Internet and Digital Citizenship, Bgelders@coface-eu.org.

Child Focus is the Belgian centre for Missing and Sexually exploited children, both online and offline. The organization is dedicated to combatting and preventing these phenomena. As the coordinator of the Safer Internet Centre in Belgium, Child Focus operates a 24/7 helpline (116 000) for all questions or problems regarding the online safety of children, as well as a hotline (abuseimages.be) for the anonymous reporting of online child sexual abuse material. Through a prevention and education program, we offer a wide range of freely accessible tools and resources for children, parents, and professionals—empowering them to create safer online experiences.

Contact point: Tijana, Policy Advisor on Child Sexual Abuse Material, Tijana.popovic@childfocus.org