

cerre

Centre on Regulation in Europe



**PROTECTION OF MINORS:
AGE-APPROPRIATE
DESIGN**

March 2025

Miriam Buiten
Christoph Busch



cerre

Issue Paper

Protection of Minors: Age-Appropriate Design

Miriam Buiten
Christoph Busch

March 2025



As provided for in CERRE's bylaws and procedural rules from its “Transparency & Independence Policy”, all CERRE research projects and reports are completed in accordance with the strictest academic independence.

The project, within the framework of which this report has been prepared, received the support and/or input of the following CERRE member organisations: Arcom, Amazon, BIPT, CnaM, EETT, Meta, Microsoft, Ofcom, Tencent. However, they bear no responsibility for the contents of this report. The views expressed in this CERRE report are attributable only to the authors in a personal capacity and not to any institution with which they are associated. In addition, they do not necessarily correspond either to those of CERRE, or of any sponsor or of members of CERRE.

© Copyright 2025, Centre on Regulation in Europe (CERRE)

info@cerre.eu – www.cerre.eu



Table of Contents

<u>ABOUT CERRE.....</u>	<u>3</u>
<u>ABOUT THE AUTHORS</u>	<u>4</u>
<u>1. INTRODUCTION</u>	<u>5</u>
<u>2. DEFINING AGE-APPROPRIATE DESIGN</u>	<u>8</u>
<u>3. GOALS OF AGE-APPROPRIATE DESIGN</u>	<u>10</u>
3.1 BROAD GOALS: THE BEST INTERESTS OF THE CHILD	10
<u>4. THE DSA’S FOCUS: ONLINE SAFETY THROUGH RISK MITIGATION</u>	<u>12</u>
4.1 RELATIONSHIP OF GUIDELINES TO DSA OBLIGATIONS	13
<u>5. RISK MITIGATION</u>	<u>16</u>
5.1 TYPES OF RISKS.....	16
5.2 TYPES OF HARM	17
<u>6. A FRAMEWORK FOR IMPLEMENTING AGE-APPROPRIATE DESIGN</u>	<u>18</u>
6.1 PRINCIPLES	18
6.2 FRAMEWORK	19
RISK-BASED APPROACH	19
LABELLING SYSTEM.....	20
6.3 EXAMPLE SCENARIOS.....	22
<u>7. OUTLOOK: TOWARDS SAFER AND CHILD-CENTRIC DIGITAL ENVIRONMENTS</u>	<u>25</u>
<u>REFERENCES</u>	<u>27</u>



About CERRE

Providing high quality studies and dissemination activities, the Centre on Regulation in Europe (CERRE) is a not-for-profit think tank. It promotes robust and consistent regulation in Europe's network and digital industry and service sectors as well as in those impacted by the digital and energy transitions. CERRE's members are regulatory authorities and companies operating in these sectors, as well as universities.

CERRE's added value is based on:

- its original, multidisciplinary and cross-sector approach covering a variety of markets, e.g., energy, mobility, sustainability, tech, media, telecom, etc.;
- the widely acknowledged academic credentials and policy experience of its research team and associated staff members;
- its scientific independence and impartiality; and,
- the direct relevance and timeliness of its contributions to the policy and regulatory development process impacting network industry players and the markets for their goods and services.

CERRE's activities include contributions to the development of norms, standards, and policy recommendations related to the regulation of service providers, to the specification of market rules and to improvements in the management of infrastructure in a changing political, economic, technological, and social environment. CERRE's work also aims to clarify the respective roles of market operators, governments, and regulatory authorities, as well as contribute to the enhancement of those organisations' expertise in addressing regulatory issues of relevance to their activities.



About the Authors



Miriam Buiten is a CERRE Research Fellow and Assistant Professor of Law and Economics at the University of St.Gallen, Switzerland. She leads a research team on “Platform Governance”, funded by the University of St.Gallen Basic Research Fund. Her research focuses on the legal issues surrounding new technologies and artificial intelligence and the role of competition law in regulating the digital economy.



Christoph Busch is Professor of Law and Director of the European Legal Studies Institute at the University of Osnabrück, Germany. He is a Fellow and Council Member of the European Law Institute (ELI) and an Affiliated Fellow at the Information Society Project at Yale University. His research focuses on consumer law, platform governance and algorithmic regulation.



1. Introduction

Protecting minors online has become an increasingly pressing issue in today's digital age. Research consistently highlights the vulnerabilities young people face when using online platforms, showing the critical need for effective protective measures. The Digital Services Act (DSA) establishes obligations for risk mitigation, opening the door to a range of potential approaches to shaping how minors interact with online platforms. As we await guidelines from the Commission by mid-2025, interest in this topic continues to grow. At the same time, the rapidly evolving landscape of regulations and platform-driven initiatives makes it challenging to get a coherent understanding of the central issues, the right questions to ask, and the most effective solutions to implement.

Children's lives increasingly take place online, bringing both opportunities and risks. With the digital environment rapidly evolving, it becomes more urgent to ensure children's protection online while enabling them to fully explore and benefit from digital services. Just as physical spaces and products for children are regulated with their safety in mind, the digital environments they engage with must also be designed to prioritise their well-being.¹ This is especially important given that children, in practice, have easy access to a vast range of online services, content, and interactions — many of which are not specifically intended for them and may not be appropriate. With online spaces often shared between children and adults, there is a clear need to build in protections to keep children safe in these mixed environments. Children should be able to benefit fully from the digital world without being exposed to addictive design, harmful content, or exploitative commercial practices.²

Much research has already been done in the field of age-appropriate design, supported by ongoing discussions like the 2024 Commission's call for input on guidance to protect minors. Building on this work, we can identify key goals and principles to create a practical and effective framework for implementing the DSA obligations. This provides clear, actionable guidance to turn these goals into meaningful protections for minors online.

This Issue Paper focuses on age-appropriate design as part of a broader safe-by-design framework, alongside age assurance, which is addressed in the accompanying DSA Forum Issue Paper. Age-appropriate design is important in complementing age assurance, as it goes beyond managing access to platforms, to ensure children's safety and positive experiences once using online services.³ While age assurance has rightfully attracted much attention, it should not be viewed as a standalone solution to online safety challenges. Instead, it is just one piece of a larger puzzle, working alongside other protective measures to create safer digital environments for children. In some cases, this broader

¹ OECD, Towards Digital Safety By Design For Children, OECD Digital Economy Papers, June 2024, No. 363, at 5, https://www.oecd.org/en/publications/towards-digital-safety-by-design-for-children_c167b650-en.html.

² Livingstone, S., Cantwell, N., Özkul, D., Shekhawat, G., & Kidron, B. (2024). The best interests of the child in the digital environment, <https://www.digital-futures-for-children.net/digitalfutures-assets/digitalfutures-documents/Best-Interests-of-the-Child-FINAL.pdf>; Atabey, A., Livingstone, S., & Pothong, K. (2023). When are commercial practices exploitative? Ensuring child rights prevail in a digital world. Digital Futures Commission, <https://eprints.lse.ac.uk/119542>.

³ While age assurance can be considered an aspect of age-appropriate online service design, this issue paper leaves it out of its scope, focusing on child protection online after they access platforms.



framework relies on age assurance to restrict children’s access to certain content or services that may pose risks. In others, the emphasis shifts to age-appropriate design and other protective measures, particularly where age assurance cannot or should not be applied. Most importantly, effective child safety strategies focus not only on access control, but also on ensuring strong protections are in place when minors do engage with online services and content. Moreover, all these measures must be proportionate and account for the rights and interests of others, such as adult users, as well.

Age-appropriate design plays a critical role on platforms, because protecting underage users requires more than blocking access to services or specific content through age assurance measures. It also involves the impact of how content is actively recommended and promoted to children. Recommender systems play a significant role in shaping children’s online experiences, with algorithms potentially amplifying harmful patterns — for example, repeatedly surfacing content that may not be illegal or inherently harmful, but becomes problematic through excessive exposure. Beyond content, children face a range of design-related risks, from autoplay features and constant notifications to deceptive design practices. These risks extend to broader issues, including privacy violations, commercial exploitation, and safety threats such as inappropriate contact from adults or fraudulent schemes. Age-appropriate design addresses these wider concerns, going well beyond the scope of age assurance alone.

While the impacts of recommender systems and platform design are not exclusive to children — and are therefore part of broader risk mitigation under the DSA — they are particularly acute for children, given their vulnerability online. Effective age-appropriate design helps to design out risks before they arise, for example through default privacy-protective settings, restrictions on targeted advertising, safeguards in recommender systems, and other child-friendly design choices. In essence, the goal is to prevent harm through thoughtful design, creating safer and more supportive online environments for children. At the same time, these measures must be proportionate and carefully balanced, taking into account other fundamental rights and broader societal interests.

This Issue Paper considers both specific design measures and broader governance mechanisms that platforms can adopt to protect children. While the paper thus takes a broad view of age-appropriate design, its primary focus is on online safety for children within the context of the DSA. It identifies risks across the 5Cs framework, including content, contact, conduct, contract, and commercial risks. These risks may include grooming, bullying, exploitation, exposure to harmful or illegal content, as well as the psychological harms caused by algorithms that amplify harmful behaviours or reinforce negative patterns.

Accordingly, this Issue Paper aims to:

- Clarify the goals of age-appropriate design in relation to obligations under the DSA related to child safety.
- Identify principles to ensure online safety for children.
- Highlight best practices that could complement DSA requirements, forming the basis for guidelines.



This Issue Paper highlights two key points central to drafting guidance on children online and advancing the ongoing discussion.

First, the **purpose of the guidance** needs to be clearly defined. It could serve two potential roles: (1) clarifying DSA obligations to support effective implementation and enforcement, and/or (2) recommending best practices that go beyond the DSA obligations. In practice, distinguishing between the two may be challenging, as the DSA's provisions on age-appropriate design are formulated generally and not specific to protection of minors.

Second, the guidance should aim to **establish a framework** that categorises risks, harms, and protective measures. This framework could clarify which measures are directly mandated by the DSA or derived from its obligations—falling under implementation guidance—and which are recommended as best practices. Additionally, the guidance should identify key principles to underpin this framework.

To kick off this work, the Issue Paper proposes guiding principles and a practical framework to make protecting children on online platforms more concrete and actionable. It focuses on putting the DSA's age-appropriate design obligations into practice while considering how they align with other legal frameworks, aiming to create safer and more age-appropriate digital spaces for children.



2. Defining Age-Appropriate Design

Age-appropriate design means tailoring digital services and platforms to align with the developmental, cognitive, and emotional needs of children and young people, while ensuring their safety, privacy, and wellbeing. This includes designing online services with children’s safety in mind, incorporating safeguards just as we do for physical products and spaces.⁴

Importantly, not all online services are specifically designed for children — yet many are frequently accessed by children. This is where the boundary between age assurance and age-appropriate design becomes relevant: services that are regularly used by children, even if not exclusively intended for them, should still incorporate appropriate protections. Creating fully separate, child-only spaces may be appropriate in some cases, but this is not a proportionate or practical solution across the board. In reality, online environments are often mixed, making it difficult to carve out clear boundaries between child and adult spaces. Combined with how easily children can access inappropriate content compared to the offline world, this means that, in practice, robust age-appropriate design is often necessary to ensure their safety in general-purpose digital spaces. Age-appropriate design seeks to create online environments that are not only safe but also empowering, allowing minors to explore, learn, and connect without unnecessary risks.⁵

Broadly, age-appropriate design encompasses:

1. **Technical measures:** Steps platforms can take to encourage safe and beneficial uses of their services while restricting harmful uses.
2. **Governance measures:** Policies and frameworks platforms implement to regulate conduct and content on their platforms.

Thus, age-appropriate design in the context of the DSA includes all ways in which platforms design, govern, and manage their services to protect and empower children. In a narrower sense, age-appropriate design focuses on the technical aspects of platform design—such as user interfaces and algorithms (including recommender systems)—that directly shape user experiences. This Issue Paper aims to provide guidance on age-appropriate design in its broadest sense, while emphasising the importance of specific design measures, particularly those relating to interfaces and algorithms.

Broadly viewed, age-appropriate design covers a wide spectrum of tools and measures aimed at ensuring the safety, privacy, and well-being of minors in digital environments. This includes factors like ensuring content is suitable, creating user-friendly interfaces, implementing privacy-focused data settings, and protecting against harmful interactions or exploitative practices. A central component is **privacy and data protection**, which involves minimising the collection of personal data, offering transparent and accessible privacy policies, and implementing robust mechanisms for obtaining

⁴ OECD, Towards Digital Safety By Design For Children, OECD Digital Economy Papers, June 2024 No. 363, at 10-12, https://www.oecd.org/en/publications/towards-digital-safety-by-design-for-children_c167b650-en.html.

⁵ See further below on Goals.



parental consent where necessary. Equally important is **content recommendation⁶ and moderation**, which should help ensure that the content accessible to minors is free from harmful or inappropriate material, providing a safer online experience. Another essential element is **user experience**, where interfaces are designed to be intuitive and easy to navigate for younger users, considering their diverse levels of literacy and cognitive understanding. Lastly, effective age-appropriate design incorporates **risk mitigation features**, such as limiting interactions with strangers, preventing exploitative or addictive behaviours, and offering tools for reporting and blocking harmful content. These combined efforts should help create a digital environment that not only protects minors but also empowers them to explore and learn safely.

⁶ Gómez, E., Charisi, V., & Chaudron, S. (2021). Evaluating Recommender Systems with and for Children: towards a Multi-Perspective Framework. In Perspectives@ RecSys.



3. Goals of Age-Appropriate Design

3.1 Broad Goals: The Best Interests of the Child

The best interests of the child must serve as the central guiding principle and starting point for age-appropriate design in online services. However, these efforts must also be carefully balanced with other important interests, such as data protection, (cyber)security, innovation, and fair competition. Safeguarding children’s best interests should complement broader legal, regulatory, and societal objectives. This balancing act takes place within the wider framework of fundamental rights and freedoms, including those of other citizens and businesses, as set out in the EU Charter of Fundamental Rights. Any measures taken should therefore be proportionate, ensuring the protection of children without imposing undue restrictions on other rights and interests.

The best interests of the child is a rights-based concept — it is dynamic, evolving, and must be assessed in relation to each individual child’s circumstances, including their age, developmental stage, personal context, and specific needs.⁷ This means there is no single, fixed definition of what best serves children’s interests online; instead, it requires careful, context-sensitive consideration.⁸ At its core, prioritising children’s best interests means **fostering positive experiences and opportunities for children online, while actively minimising the risks of harm**. This approach is essential to ensuring children can benefit from the digital environment, not just be protected from it.

Protecting children online thus requires taking a holistic approach to their rights—not just safety and security but also freedom of expression and access to content.⁹ A child-centred approach avoids seeing children only as vulnerable victims or prioritising their protection from risk at the expense of their online opportunities.¹⁰ Instead, it recognises children as active participants in the digital world while ensuring they are not unfairly held responsible for online risks or potential harm to themselves or others.¹¹ Prioritising the best interests of the child means enabling their access to the digital world in ways that allow them to fully enjoy their rights and freedoms.¹²

⁷ General comment No. 14 on the right of the child to have his or her best interests taken as a primary consideration (art. 3, para. 1), UN Committee on the Rights of the Child (2013). See further Livingstone, S., Cantwell, N., Özkul, D., Shekhawat, G., & Kidron, B. (2024). The best interests of the child in the digital environment, <https://www.digital-futures-for-children.net/digitalfutures-assets/digitalfutures-documents/Best-Interests-of-the-Child-FINAL.pdf>.

⁸ General comment No. 20 on the implementation of the rights of the child during adolescence, UN Committee on the Rights of the Child (2016).

⁹ COE Handbook for policy makers on the rights of the child in the digital environment at 39-40, <https://rm.coe.int/publication-it-handbook-for-policy-makers-final-eng/1680a069f8>

¹⁰ Staksrud, E. & Livingstone, S. (2009). Children and online risk: Powerless victims or resourceful participants? *Information, Communication and Society*, 12(3): 364–387. <http://eprints.lse.ac.uk/30122/>

¹¹ 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. <https://doi.org/10.21241/ssoar.71817>.

¹² COE Handbook for policy makers on the rights of the child in the digital environment at 37, <https://rm.coe.int/publication-it-handbook-for-policy-makers-final-eng/1680a069f8>



Consequently, a comprehensive approach to age-appropriate design should also seek to **promote positive experiences**, such as access to educational and diverse content and tools that foster healthy social development. Children's safety and security are critical, but their right to explore, engage, and access enriching online experiences should not be overlooked.

Striking the right balance between these rights means considering societal interests and ensuring interventions are fair and proportionate.¹³ At the same time, in the current regulatory context, guidance on creating a safer online environment for children must address the default state of unrestricted access and use of online services. This shifts the focus toward their safety and wellbeing when defining concrete measures for child protection. While a child's right to freedom of expression is important, it is not absolute or more important than other rights, such as privacy, protection from harmful content, safety from violence, and the right to health, play, and development.¹⁴ Since the digital space is mostly designed for adults and often sexualised, polarised, and commercialised, it creates significant challenges for children's safety and wellbeing.¹⁵ To truly support children's right to self-expression and enjoyment of online opportunities, digital environments must recognise and protect them as distinct users, ensuring they can express themselves while staying properly protected.¹⁶

- In practical terms, guidance on protecting minors should aim to for the following: **Ensuring children's safety and well-being**: Creating digital environments that protect children from harm, including exposure to inappropriate content, exploitation, and other online risks.
- **Promoting positive experiences**: Designing platforms and services that enable children to learn, connect, and thrive in ways that respect their developmental needs and capacities.
- **Upholding children's rights**: Ensuring that children's privacy, autonomy, and other rights are respected, in line with principles like those outlined in the UN Convention on the Rights of the Child.¹⁷
- **Encouraging responsibility among platforms**: Establishing expectations that platforms proactively consider the needs of children in their design and operational choices.

¹³ Green, A., Wilkins, C., & Wyld, G. (2019). Keeping children safe online. Nominet, NPC, <https://www.thinknpc.org/wp-content/uploads/2019/07/Keeping-Children-Safe-Online-NPC-Nominet-ParentZone-2019.pdf>. See for differences in national approaches to balancing opportunities and risks for children online Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., and Hasebrink, U. (2020). EU Kids Online 2020: Survey results from 19 countries. EU Kids Online. <https://doi.org/10.21953/lse.47fdeqj01ofo>.

¹⁴ 5Rights Foundation (2019). Towards an internet safety strategy. 5Rights. <https://5rightsfoundation.com/uploads/final-5rightsfoundation-towards-an-internet-safety-strategyjanuary-2019.pdf>

¹⁵ 5Rights Foundation (2019). Towards an internet safety strategy. 5Rights. <https://5rightsfoundation.com/uploads/final-5rightsfoundation-towards-an-internet-safety-strategyjanuary-2019.pdf>

¹⁶ 5Rights Foundation (2019). Towards an internet safety strategy. 5Rights. <https://5rightsfoundation.com/uploads/final-5rightsfoundation-towards-an-internet-safety-strategyjanuary-2019.pdf>

¹⁷ And further elaborated in General comment No. 25 on children's rights in relation to the digital environment, UN Committee on the Rights of the Child (2021).



4. The DSA's Focus: Online Safety through Risk Mitigation

The DSA addresses the protection of minors through a dedicated article on minors, alongside broader risk management obligations for VLOPs that also concern minors. These provisions aim to improve the protection of minors by establishing specific requirements for online platforms. Platforms are required to take **proportionate measures** to address risks related to content, conduct, contact, and consumer issues. However, the key question remains: **what is a reasonable expectation of platforms in terms of their concrete role and responsibility in managing these risks?**

Concretely, the DSA requires the following:

- **Art. 14 DSA on terms and conditions:** Article 14(3) DSA obligates intermediary service providers to ensure that their terms and conditions are both accessible and understandable to minors.
- **Art. 28 DSA on online protection of minors:** Article 28 requires platforms to adopt appropriate and proportionate measures to ensure a high level of privacy, safety, and security for minors using their services.
 - Preamble Paragraph 71 elaborates on this by emphasising the need for online interfaces to be designed with the highest standards of privacy, safety, and security for minors by default, where appropriate. Platforms may also adopt standards, participate in codes of conduct, or use available guidance instruments to ensure they follow best practices for protecting minors. Additionally, platforms must avoid presenting advertisements based on profiling when they have reasonable certainty that the recipient is a minor and should minimise the collection and processing of minors' data.
 - Preamble Paragraph 89 further specifies that very large online platforms (VLOPs) and search engines must prioritise the best interests of minors. This includes adapting their service design and interface, especially for services targeted at or predominantly used by minors. These platforms must ensure minors can easily access regulatory mechanisms such as notice-and-action systems and complaint tools. They should also take measures to protect minors from content that could harm their physical, mental, or moral development, providing tools for limiting access to such content. It is highlighted again that platforms may consider industry best practices, including self-regulatory codes of conduct and guidelines issued by the Commission, in implementing these measures.
- **Arts. 34-35 DSA on risk assessment and mitigation:** Article 34 mandates that VLOPs conduct risk assessments to evaluate how their services affect minors. These assessments must address the spread of harmful content, risks of online harassment, and exposure to age-inappropriate advertising. Article 35 requires platforms to take concrete steps to mitigate these risks, such as improving content moderation, increasing privacy controls, and



implementing stricter age verification systems. However, the DSA does not prescribe specific mitigation measures for each identified risk. While it offers examples of potential mitigations, it does not mandate any particular approach. Furthermore, the DSA does not specify when or if these potential measures would be appropriate or proportionate. As a result, there is a clear need for further guidance on this matter.

- Preamble Paragraph 81 urges VLOPs to consider how easily minors can understand the design and operation of the service and the potential risks posed by content that could harm their health, physical, mental, or moral development. These risks may stem from interface designs that exploit minors' inexperience or vulnerabilities, either intentionally or unintentionally, or that encourage addictive behaviours.

4.1 Relationship of Guidelines to DSA Obligations

A guidance on age-appropriate design can serve two complementary purposes:

- **Implementation of DSA Obligations:** Providing practical guidance on how enforceable obligations, such as those in Article 28 DSA, can be put into action. This includes outlining specific measures platforms must take to comply and ensuring clarity around obligations to aid enforcement.
- **Recommendations for Best Practices:** Suggesting broader strategies that go beyond the minimum legal requirements, encouraging platforms to take a proactive approach in innovating and implementing measures that prioritise children's safety and well-being.

By providing guidance to bridge the gap between the DSA's broad provisions and the practical steps needed to protect minors, regulators could help establish clearer, enforceable standards while encouraging platforms to go beyond minimum requirements in protecting children online.¹⁸

When it comes to setting clear standards, one key area requiring further clarity is when and how VLOPs should act to mitigate risks linked to harmful — but legal — content. While the DSA primarily targets illegal content, it also addresses harmful content indirectly through its risk assessment and mitigation obligations. The DSA deliberately does not define harmful content. This reflects the legislator's decision to leave the definition of illegal content — and the boundary between legal and illegal material — to Member States. Moreover, explicitly requiring platforms to remove harmful but legal content would raise serious freedom of expression concerns. Instead, the DSA takes a procedural approach to harmful content: it focuses not on mandating removal, but on requiring platforms to assess and mitigate risks arising from harmful content, particularly for minors. This procedural focus means platforms are not legally obliged to take down harmful content as a rule — but they are required to identify risks, assess how their services contribute to those risks, and take appropriate mitigation measures. This leaves platforms in a challenging position when implementing the DSA: in

¹⁸ See also 5Rights Feedback Commission Consultation Protection of minors – guidelines, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14352-Protection-of-minors-guidelines/F3496663_en.



practice, they need to decide for themselves when certain content is sufficiently harmful to trigger their risk mitigation obligations. This raises critical implementation questions:

- How should platforms determine when content poses a risk to minors?
- What specific measures are required to mitigate those risks, short of removing the content entirely?

Without clearer guidance on these questions, platforms face uncertainty in balancing their obligations to protect minors with their responsibilities to respect freedom of expression and avoid over-removal of legal content. This highlights the need for practical, proportionate, and context-sensitive guidance that clarifies what platforms are expected to do in these cases to meet their obligations under the DSA. The guidelines could play a key role in explaining how platforms should apply Articles 28 and 34-35 in practice, helping them navigate the risk-based approach the DSA promotes, particularly when safeguarding children. At the same time, the guidance should respect the DSA approach that needs to be sufficiently flexible to cover a wide variety of risks, which will inevitably differ across platforms and services.

In this context, it is important to clearly distinguish between platforms' legal responsibilities under the DSA and aspirational recommendations that the guidelines may offer on top of these obligations. Alongside interpreting the DSA's enforceable requirements, the guidelines could also offer additional, non-binding recommendations — providing platforms with a best practice framework that goes beyond the minimum legal obligations under the DSA.

The primary purpose of the guidance is to provide clarity on how the DSA's obligations will be interpreted and enforced in practice. Yet, given that the DSA's provisions on the protection of minors and risk mitigation are broad and open-ended, the European Commission has significant discretion in shaping how far-reaching the concrete measures required under the DSA should be — including measures affecting platform design and governance mechanisms. In other words, because the DSA leaves room for interpretation, the guidelines will play a central role in shaping its practical implementation by setting expectations for the specific steps platforms must take.

As the guidance process moves forward, it is essential to clarify whether the guidelines will focus solely on interpreting binding obligations under the DSA, or whether they will also include voluntary recommendations that exceed what the DSA legally requires. This distinction is particularly important given the open-ended and novel nature of the DSA's provisions.

In particular, it will be important to determine whether provisions such as Article 28 can be interpreted to mandate specific protective measures — with the guidelines fleshing out what those measures should be — or where the guidelines are intended primarily to suggest good practices that platforms may choose to adopt beyond their legal duties.

In addition to offering clear, practical guidance for online platforms on how to meet their obligations under the DSA and establishing best practices through recommendations, the guidelines could also provide a **framework to help platforms ask the right questions** during their risk assessments for



children's access to and use of their services.¹⁹ Initial steps toward developing such a framework are outlined further below.

¹⁹ See also 5Rights Feedback Commission Consultation Protection of minors – guidelines, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14352-Protection-of-minors-guidelines/F3496663_en.



5. Risk Mitigation

5.1 Types of Risks

The concept of risk mitigation for minors encompasses four key areas:²⁰

- **Content risks:** Exposure to harmful or age-inappropriate material.
- **Conduct risks:** Risks stemming from a child’s own behaviour online, such as oversharing personal information.
- **Contact risks:** Potential dangers from interactions with strangers or harmful individuals.
- **Consumer risks:** Exploitation through targeted advertising or manipulative design that encourages excessive engagement.

Recognising the interplay between various types of online risks—content, conduct, contact, and consumer—is important because these risks often overlap and reinforce each other, amplifying their potential harm to children. For example, harmful content may lead to risky conduct, such as imitating dangerous behaviours, or expose children to harmful contact, like online predators.²¹ Similarly, consumer risks, such as exploitative in-app purchases, can expose users to inappropriate content or manipulative advertising. Therefore, child protection measures must address these risks through a comprehensive approach to provide effective protections for young users.

Not all risks faced by minors are directly covered by the DSA’s obligations. In particular, broader consumer protection issues that are especially relevant for minors may be dealt with outside the DSA framework. The recently published Digital Fairness Fitness Check Report highlights that children and young people are particularly vulnerable to certain commercial practices, such as in-game and in-app purchases, including virtual items like loot boxes, as well as the increasing use of gamification techniques in online retail environments. Additionally, the use of alternative in-app currencies in games and apps reduces price transparency, making it harder for young consumers to understand the real-world cost of their purchases. This practice also reduces the so-called “pain of paying,”²² undermining children’s ability to self-regulate their spending and encouraging impulsive purchases.

In sum, while age-appropriate design under the DSA should take account of the 4Cs, it is equally important to recognise the broader legislative framework, which addresses some of these risks through consumer protection, data protection, and other relevant laws.

²⁰ 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. <https://doi.org/10.21241/ssoar.71817>.

²¹ 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. <https://doi.org/10.21241/ssoar.71817>.

²² On the concept of “pain of paying” see Drazen Prelec and George Loewenstein, The Red and the Black: Mental Accounting of Savings and Debt, *Marketing Science* 17(1)(1998): 4-28.



5.2 Types of Harm

The likelihood and severity of harmful outcomes for children online depend on multiple factors. These include the nature of the risk itself, such as its probability and potential consequences, and the design, regulation, and management of the digital environment, including features like privacy settings, content moderation, and access to support services.²³ Additionally, a child's unique circumstances play a role, as what may be harmful to one child might not affect another in the same way. These differences are shaped by broader societal factors—such as cultural norms, regulatory frameworks, political priorities, economic resources, and education systems—as well as individual characteristics like age, gender, digital skills, resilience, personality, socio-economic background, and family context.²⁴

Specific harms to minors online encompass a range of physical, psychological, and developmental risks. Physical harm can arise from exposure to content encouraging self-harm or dangerous behaviours, putting children at direct risk.²⁵ Psychological and developmental harm may result from violent content,²⁶ bullying, or the influence of recommender systems,²⁷ where they amplify problematic material by repeatedly pushing similar content personalised for children.²⁸ Additionally, exposure to inappropriate content, such as adult material, and the promotion of addictive behaviours further threaten children's healthy development and well-being.²⁹

²³ 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. <https://doi.org/10.21241/ssoar.71817>.

²⁴ 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. <https://doi.org/10.21241/ssoar.71817>.

²⁵ Lan, Y. T., Pan, Y. C., & Lin, Y. H. (2022). Association between adolescents' problematic online behaviors and self-harm risk. *Journal of affective disorders*, 317, 46-51; Memon, A. M., Sharma, S. G., Mohite, S. S., & Jain, S. (2018). The role of online social networking on deliberate self-harm and suicidality in adolescents: A systematised review of literature. *Indian journal of psychiatry*, 60(4), 384-392.

²⁶ Medietilsynet, Robust, resigned or numb? – Interviews with young people and parents about harmful content online, 2024,

https://www.medietilsynet.no/globalassets/dokumenter/rapporter/240205_robust_resignert_nummen.pdf

²⁷ See for an overview Wood, S. (2024). Children and Social Media Recommender Systems: How Can Risks and Harms be Effectively Assessed in a Regulatory Context?. Available at SSRN 4978809.

²⁸ Stem4. (2022). Body image among young people: Negative perceptions and damaging content on social media, combined with pandemic fallout, contribute to a low sense of self-worth and a rise in eating difficulties, new survey reveals. <https://stem4.org.uk/wpcontent/uploads/2022/12/Body-image-among-young-people-Negative-perceptions-anddamaging-content-on-social-media...-new-survey-reveals-Dec-22.pdf>; Hilbert, M., Cingel, D. P., Zhang, J., Vigil, S. L., Shawcroft, J., Xue, H., ... & Shafiq, Z. (2023). # BigTech@ Minors: Social Media Algorithms Personalize Minors' Content After a Single Session, but Not for Their Protection. Available at SSRN 4674573. See further Broughton Micova, S., Schnurr, D., Calef, A., Enstone, B. CERRE Report, Cross-cutting Issues for DSA Systemic Risk Management: An Agenda for Cooperation, July 2024, at 42, <https://cerre.eu/publications/cross-cutting-issues-for-dsa-systemic-risk-management-an-agenda-for-cooperation/>.

²⁹ Bozzola, E., Spina, G., Agostiniani, R., Barni, S., Russo, R., Scarpato, E., ... & Staiano, A. (2022). The use of social media in children and adolescents: Scoping review on the potential risks. *International journal of environmental research and public health*, 19(16), 9960; Al-Samarraie, H., Bello, K. A., Alzahrani, A. I., Smith, A. P., & Emele, C.



6. A Framework for Implementing Age-Appropriate Design

6.1 Principles

Building on the identified goals of age-appropriate design, the central DSA obligations for protecting minors, and the focus on mitigating risks and harm, we can outline the following principles for implementing the DSA's provisions on protecting minors. These principles may also serve as a foundation for shaping the forthcoming Commission guidance:

Best Interests of the Child: Ensure that children's well-being, rights, and needs are the primary consideration in the digital environment, striking a balance between maximising opportunities and minimising risks online. This principle should be applied within the broader framework of fundamental rights and freedoms that govern different online services.

Proactive strategies: Anticipate and address vulnerabilities before they emerge, preventing potential harm to children.

- **Privacy and Data Protection:** Minimise the collection and processing of children's personal data, ensuring it is collected and used responsibly.³⁰ **Transparency:** Clearly communicate terms and conditions in a way that children and their guardians can understand,³¹ as well as transparent information on risk and actual harm that has occurred on the service.³²
- **Safety in Functionalities:** Design platform features to account for safety, minimising risks like harmful interactions or exposure to inappropriate content.
- **Encouraging Safe Behaviour through Design:** Use design elements that nudge children toward safe and healthy online behaviours, avoiding harmful persuasive techniques or "dark patterns" that compromise their privacy, safety, or well-being, or foster addictive behaviours.³³

(2022). Young users' social media addiction: causes, consequences and preventions. *Information Technology & People*, 35(7), 2314-2343.

³⁰ COE Handbook for policy makers on the rights of the child in the digital environment at 45-46, <https://rm.coe.int/publication-it-handbook-for-policy-makers-final-eng/1680a069f8>

³¹ UNCRC General comment No. 25, Para. 39; DSA Article 14(3); UK ICO (2020) Principle 4; Irish DPC (2021) Chapter 3; 5Rights Foundation (2021) Tick to Agree: Age appropriate presentation of published terms, <https://5rightsfoundation.com/resource/tick-to-agree-age-appropriate-presentation-of-published-terms/>.

³² OECD, 13-14.

³³ 5Rights (2023) Disrupted Childhood: The cost of persuasive design, <https://5rightsfoundation.com/resource/updated-report-disrupted-childhood-the-cost-of-persuasive-design/>; 5Rights (2021) Pathways: How digital design puts children at risk, <https://5rightsfoundation.com/wp-content/uploads/2021/09/Pathways-how-digital-design-puts-children-at-risk.pdf>; UNCRC General comment No. 25, Para. 110; European Parliament (2023) Resolution on addictive design of online services and consumer protection in the EU single Market, https://www.europarl.europa.eu/doceo/document/TA-9-2023-0459_EN.html.



- **Safe Defaults:** Ensure safety is embedded by default in design choices:³⁴
 - **Privacy Defaults:** Set privacy settings, such as children’s profiles, to “high privacy” unless a compelling reason aligns with the best interests of the child.³⁵
 - **Engagement Design:** Avoid or disable features aimed at maximising engagement or time spent on the platform, such as autoplay, endless scroll, random rewards, popularity metrics, or techniques that induce time pressure or anticipation.³⁶
- **Content Moderation and Governance:** Maintain robust content moderation and governance practices to protect minors, both by setting clear rules for content and conduct on the platform and by enforcing them effectively.

6.2 Framework

Based on these principles, we can outline a potential framework for age-appropriate design structured around three key tiers:

- **Best Practices:** Industry-accepted measures that align with the best interests and developmental needs of children, such as strong privacy-by-default settings, transparent data policies, and age-appropriate content moderation.
- **Grey Practices:** Practices that may be acceptable in certain contexts but require close monitoring to ensure they do not cause harm. These could include personalised content recommendations or limited data collection, which must be carefully implemented to protect minors.
- **Bad Practices:** Clearly harmful or exploitative practices that should be outright prohibited, such as manipulative design tactics (dark patterns) targeting minors, excessive data harvesting, or inappropriate advertising.

Risk-based Approach

Such a framework can be helpful in structuring risks and categorising measures, and offering concrete suggestions for technologies to be used and measures to be taken.³⁷

³⁴ 5Rights Foundation (2019). Towards an internet safety strategy, <https://5rightsfoundation.com/wp-content/uploads/2024/10/final-5rights-foundation-towards-an-internet-safety-strategy-january-2019.pdf>.

³⁵ French CNIL (2021), Recommendation 8; Irish DPC (2021), Fundamental 14; UK ICO (2020), Principle 7; Dutch Ministry of the Interior (2021), Principle 6; Swedish Authorities, (2021), Chapter 2.6.

³³ European Commission (Accessed 2023) What does data protection ‘by design’ and ‘by default’ mean?.

³⁶ 5Rights 2024, A High Level of Privacy, Safety & Security for Minors: A best practices baseline for the implementation of the Digital Services Act for children, <https://5rightsfoundation.com/resource/a-high-level-of-privacy-safety-security-for-minors/>; 5Rights (2021) Pathways: How digital design puts children at risk, <https://5rightsfoundation.com/wp-content/uploads/2021/09/Pathways-how-digital-design-puts-children-at-risk.pdf>.

³⁷ See further e.g. IEEE Standard for an Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children," in IEEE Std 2089-2021 , vol., no., pp.1-54, 30 Nov. 2021, doi: 10.1109/IEEESTD.2021.9627644; CEN-CENELEC CWA on Age Appropriate Design, CWA 18016:2023, 2023.



Many potential measures for protecting children online can be effective or problematic depending on how they are designed and applied. Therefore, their risks and benefits must be carefully evaluated, calling for a nuanced, risk-based approach that considers both intended protections and potential unintended consequences.

Importantly, while it can be useful to assess individual platform features or practices in isolation, it is essential for enforcement to also evaluate their combined effects. Certain features — such as recommendation algorithms, autoplay functions, and reward mechanisms — may amplify risks when they interact or reinforce each other, creating a cumulative impact that is greater than the sum of its parts. The guidance should make this explicit, emphasising that enforcement efforts under the DSA will consider not only individual features but also their combined and overall impact on children’s safety and well-being.

The table provided below is not intended to be exhaustive or definitive but serves as guidance rather than a final judgment on these measures. Implementation must be context-sensitive, avoiding premature conclusions about what will work universally. Additionally, there is a risk that measures may be implemented superficially to “check the box” without achieving meaningful change or genuinely enhancing the protection of minors. To provide clarity, possible scenarios with concrete examples of both good and bad practices are included further below.

While implementation is necessarily platform-specific and tailored to risk, a structured framework can be helpful for identifying the types of settings or measures to prioritise when considering age-appropriate design. Such a framework helps ensure that the obligations under the DSA translate into concrete, impactful changes in platform design. Since the DSA’s provisions in this area are relatively broad and open-ended, much of the responsibility for enforcement lies with regulators. A well-thought-out framework can provide clarity and focus for these efforts while leaving room for context-specific interpretation.

To illustrate this, the table below includes examples of best practices and potential pitfalls in implementing these measures. It highlights what successful implementation looks like and what practices to avoid, fostering meaningful and effective protection for minors.

Labelling System

To improve transparency and accountability, the framework could be complemented by introducing a labelling system, such as a “Child-Safe Certified” designation. This certification would act as a visible marker, signalling that a platform has met rigorous, clearly defined standards for child protection. Such a system would empower parents and young users by providing them with a reliable way to identify platforms that prioritise the safety, privacy, and well-being of children. This designation could become a benchmark for trustworthiness in the digital ecosystem, helping users make more informed decisions about where children can engage safely online.

Such a labelling system could be integrated into the DSA framework and linked to DSA compliance, providing platforms with the opportunity to obtain a “Child-Safe Certified” status. This certification



could be anchored in well-documented best practices, serving as baseline criteria for qualification. These best practices could cover the areas outlined in **Table 1** below, and draw from the Commission guidelines on child protection.

The “Child-Safe Certified” label could also be integrated into broader public awareness campaigns, encouraging both users and platforms to prioritise child safety online. Over time, the designation might influence market dynamics, as certified platforms would gain a competitive edge by demonstrating their commitment to protecting minors.

Table 1: A Best-Practices Framework for Age-Appropriate Design of Online Platforms

	Best practices	Grey practices	High-risk practices
Terms and conditions	Age restrictions; Parental consent; Clear codes of conduct; Clear and accessible to children	Broad data collection; Monetisation from minors; unclear moderation policies	Lack of moderation policies or age restrictions; Deceptive practices
Default settings	Geolocation and camera access disabled by default	Optional personalised settings with parental approval	Location sharing or public profiles by default
Recommender systems	Promoting diverse, age-appropriate content and contacts; Tools to adjust content	Non-targeted advertisement	Recommending inappropriate content (e.g. violence, adult content, gambling, self-harm) or contacts
Interface design	Clear navigation; rewarding behaviour in child’s best interests	Persuasive design elements	Dark patterns encouraging addictive usage or purchases
Data privacy & security	Data minimisation; Encryption	Anonymised tracking of usage for performance optimisation	Selling or sharing children’s data with third parties
Parental controls & child autonomy	User-friendly parental monitoring dashboards; Age-adaptive autonomy settings	Tracking features requiring parental opt-in	Invasive monitoring that undermines children's sense of privacy
Behavioural nudges	Break reminders; encouraging educational activities	Suggestive prompts for engagement	Manipulative engagement prompts



6.3 Example Scenarios

Building on the best-practices approach and the various categories of measures, several examples of concrete measures can be outlined. These examples should allow the guidance to provide clear, concrete measures to ensure effective implementation of the DSA obligations, while allowing for enough flexibility to ensure they remain practical and adaptable for platforms of different sizes and capacities.

Terms and Conditions		
<p>Best Practice: A social media app explicitly outlines its terms and conditions using simple, age-appropriate language, including clear guidelines for acceptable behaviour and parental consent for account creation. For instance, it provides a visual walkthrough of its moderation policies and ensures no monetization of minors' data.</p>	<p>Grey Practice: A gaming platform collects broad user data for targeted advertising but anonymises the data before use. The terms and conditions mention data collection but fail to clearly explain how minors' data will be protected, leaving parents uncertain about privacy implications.</p>	<p>High-Risk Practice: A video platform has no clear terms for age restrictions or parental consent. Its unclear policies allow monetization from minors through in-app purchases and poorly define content moderation, exposing children to potentially harmful interactions.</p>

Default Settings		
<p>Best Practice: A children's app disables geolocation and camera access by default. Profiles are set to private automatically, and parental approval is required to activate optional features like chat functions.</p>	<p>Grey Practice: A video-sharing platform allows geolocation and public profiles by default but provides options for parents to disable these settings. While this offers flexibility, it places the burden on parents to ensure safety.</p>	<p>High-Risk Practice: A messaging app for children shares user location and sets profiles to public by default. These settings expose young users to privacy risks and potential harm, with minimal oversight from guardians.</p>

Recommender Systems		
<p>Best Practice: A video platform for children curates diverse, age-appropriate content and provides tools for parents and</p>	<p>Grey Practice: A gaming site shows non-targeted advertisements to users, including older children. While the ads aren't</p>	<p>High-Risk Practice: A music-streaming app recommends inappropriate content, such as explicit lyrics or videos with violent themes,</p>



children to adjust content preferences. It also excludes advertising or sensitive topics like gambling or violence.	inappropriate, they lack tailoring to children’s age groups, potentially exposing younger users to irrelevant or slightly confusing content.	based on user activity without sufficient safeguards for younger users.
---	--	---

Interface Design		
<p>Best Practice: An educational app uses a clean, intuitive interface, rewarding children for completing learning activities with fun but non-addictive features like badges or avatars.</p>	<p>Grey Practice: A gaming platform employs persuasive design elements, such as bright colours and sound effects, to encourage longer gameplay sessions. While not explicitly harmful, these designs can promote excessive screen time.</p>	<p>High-Risk Practice: An e-commerce app for children uses dark patterns, such as misleading buttons or “one-click” purchases, encouraging children to make unintended or frequent in-app purchases.</p>

Data Privacy & Security		
<p>Best Practice: A social media app implements data minimization, collecting only necessary data, encrypting it, and ensuring it is deleted after use. It clearly informs parents about the type and duration of data storage.</p>	<p>Grey Practice: An online platform tracks anonymised user behaviour to optimise app performance but does not explicitly disclose this in its privacy settings, leaving room for mistrust.</p>	<p>High-Risk Practice: A video platform sells children’s data, including browsing habits, to third parties for marketing purposes. This not only violates privacy laws but also compromises the safety of minors.</p>

Parental Controls & Child Autonomy		
<p>Best Practice: A monitoring app provides an easy-to-use parental dashboard and age-adaptive autonomy settings that balance oversight with increasing independence as children grow older.</p>	<p>Grey Practice: A children’s tracker app requires parental opt-in for monitoring features like location sharing but does not allow children to customise or disable these settings as they age, potentially undermining trust.</p>	<p>High-Risk Practice: An e-commerce app offers invasive monitoring, such as constant live camera access, without regard for the child’s privacy or autonomy, leading to an overreach into their personal space.</p>

Behavioural Nudges		
Best Practice:	Grey Practice:	High-Risk Practice:



Protection of Minors: Age-Appropriate Design

<p>A mindfulness app for children provides regular break reminders and gamifies educational activities to encourage balanced usage and meaningful engagement.</p>	<p>A gaming app uses suggestive nudges, such as “Keep playing to unlock rewards,” which increase engagement but do not cross into manipulation.</p>	<p>A social media platform employs manipulative prompts like, “Your friends are online, don’t miss out!” to pressure children into prolonged use, promoting addictive behaviour.</p>
---	---	--



7. Outlook: Towards Safer and Child-Centric Digital Environments

In anticipation of the Commission’s forthcoming guidance on the protection of minors, several key issues must be thoughtfully discussed and addressed. This Issue Paper has highlighted three main areas of focus.

First, it is essential to **clearly distinguish between the binding obligations under the DSA and any additional guidance** or recommendations provided through the guidelines. While the guidelines can — and likely should — go beyond simply interpreting the DSA’s requirements by offering broader best practice guidance, it must be clear to platforms which measures are legally required to comply with the DSA, and which are recommended but not enforceable.

This clarity is not just important for legal certainty; it is also critical to give the DSA real impact, ensuring it **drives meaningful improvements in the online environment for children**. Clear and actionable guidelines are needed to define industry best practices and help platforms understand their responsibilities under the DSA. While non-binding recommendations can encourage innovation and allow for flexible application to the wide variety of platforms, they are not sufficient on their own. Given the significant risks children face online, certain protective measures must be made mandatory. Platforms — many of which generate substantial revenue from underage users — cannot be expected to self-regulate effectively through voluntary action alone. To ensure a consistent baseline of protection, the DSA must translate key child protection expectations into concrete, enforceable measures that address the most serious risks.

Second, **establishing clear design and governance principles** is fundamental to creating safe digital environments for minors. Default settings should prioritise safety, such as implementing high-privacy configurations for children’s accounts. Additionally, design principles must actively prevent harmful patterns, such as features that foster addictive behaviours or exploit vulnerabilities. By embedding these principles into platform operations, meaningful protection and accountability can be achieved, laying the foundation for a safer and more ethical online space for minors.

Finally, there is a need to **develop a robust framework for protective measures**. Such a framework would provide structure for evaluating and implementing initiatives that prioritise children’s safety and rights effectively. Key considerations would include platforms’ terms and conditions, interface design and defaults, recommender systems, and privacy protections. By setting clear standards, this framework would establish a baseline and best practices for child protection across platforms, while allowing for flexibility to address the diverse nature of online services and risks. A “Child-Safe Certified” designation or similar labelling system could help reinforce these best practices, gradually establishing them as the industry standard for child protection online.

By addressing these issues, the Commission’s guidance can offer much-needed clarity and direction, helping to close existing gaps in the digital landscape and ensuring the protection of children’s well-



being in the online world. As this Issue Paper has emphasised, a holistic approach must be taken—one that not only protects children from inappropriate content, exploitation, and other online risks but also promotes positive experiences and supports their developmental needs. Platforms should be designed to encourage learning, creativity, and meaningful connection within a safe environment. This approach must align with fundamental principles such as those outlined in the UN Convention on the Rights of the Child, particularly with regard to privacy protection, autonomy, and enabling active participation in the digital world. Clear guidance on DSA obligations for protecting minors will help set expectations for platforms to prioritise children’s needs in their design, policies, and operations, fostering a culture of responsibility, transparency, and accountability.



References

- 5Rights (2021) Pathways: How digital design puts children at risk, <https://5rightsfoundation.com/wp-content/uploads/2021/09/Pathways-how-digital-design-puts-children-at-risk.pdf>.
- 5Rights (2023) Disrupted Childhood: The cost of persuasive design, <https://5rightsfoundation.com/resource/updated-report-disrupted-childhood-the-cost-of-persuasive-design/>.
- 5Rights 2024, A High Level of Privacy, Safety & Security for Minors: A best practices baseline for the implementation of the Digital Services Act for children, <https://5rightsfoundation.com/resource/a-high-level-of-privacy-safety-security-for-minors/>.
- 5Rights Feedback Commission Consultation Protection of minors – guidelines, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14352-Protection-of-minors-guidelines/F3496663_en.
- 5Rights Foundation (2019). Towards an internet safety strategy, <https://5rightsfoundation.com/wp-content/uploads/2024/10/final-5rights-foundation-towards-an-internet-safety-strategy-january-2019.pdf>.
- 5Rights Foundation (2021) Tick to Agree: Age appropriate presentation of published terms, <https://5rightsfoundation.com/resource/tick-to-agree-age-appropriate-presentation-of-published-terms/>.
- Al-Samarraie, H., Bello, K. A., Alzahrani, A. I., Smith, A. P., & Emele, C. (2022). Young users' social media addiction: causes, consequences and preventions. *Information Technology & People*, 35(7), 2314-2343.
- Atabey, A., Livingstone, S., & Pothong, K. (2023). When are commercial practices exploitative? Ensuring child rights prevail in a digital world. Digital Futures Commission, <https://eprints.lse.ac.uk/119542>.
- Bozzola, E., Spina, G., Agostiniani, R., Barni, S., Russo, R., Scarpato, E., ... & Staiano, A. (2022). The use of social media in children and adolescents: Scoping review on the potential risks. *International journal of environmental research and public health*, 19(16), 9960;
- Broughton Micova, S., Schnurr, D., Calef, A., Enstone, B. CERRE Report, Cross-cutting Issues for DSA Systemic Risk Management: An Agenda for Cooperation, July 2024, <https://cerre.eu/publications/cross-cutting-issues-for-dsa-systemic-risk-management-an-agenda-for-cooperation/>.
- CEN-CENELEC CWA on Age Appropriate Design, CWA 18016:2023, 2023, <https://standards.cencenelec.eu/>.
- COE Handbook for policy makers on the rights of the child in the digital environment, <https://rm.coe.int/publication-it-handbook-for-policy-makers-final-eng/1680a069f8>.
- Drazen Prelec and George Loewenstein, The Red and the Black: Mental Accounting of Savings and Debt, *Marketing Science* 17(1)(1998): 4-28.



- European Parliament (2023) Resolution on addictive design of online services and consumer protection in the EU single Market, https://www.europarl.europa.eu/doceo/document/TA-9-2023-0459_EN.html.
- Gómez, E., Charisi, V., & Chaudron, S. (2021). Evaluating Recommender Systems with and for Children: towards a Multi-Perspective Framework. In Perspectives@ RecSys.
- Green, A., Wilkins, C., & Wyld, G. (2019). Keeping children safe online. Nominet, NPC, <https://www.thinknpc.org/wp-content/uploads/2019/07/Keeping-Children-Safe-Online-NPC-Nominet-ParentZone-2019.pdf>.
- Hilbert, M., Cingel, D. P., Zhang, J., Vigil, S. L., Shawcroft, J., Xue, H., ... & Shafiq, Z. (2023). #BigTech@ Minors: Social Media Algorithms Personalize Minors' Content After a Single Session, but Not for Their Protection. Available at SSRN 4674573.
- IEEE Standard for an Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children," in IEEE Std 2089-2021 , vol., no., pp.1-54, 30 Nov. 2021, doi: 10.1109/IEEESTD.2021.9627644.
- Lan, Y. T., Pan, Y. C., & Lin, Y. H. (2022). Association between adolescents' problematic online behaviors and self-harm risk. *Journal of affective disorders*, 317, 46-51.
- 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. <https://doi.org/10.21241/ssoar.71817>.
- Livingstone, S., Cantwell, N., Özkul, D., Shekhawat, G., & Kidron, B. (2024). The best interests of the child in the digital environment, <https://www.digital-futures-for-children.net/digitalfutures-assets/digitalfutures-documents/Best-Interests-of-the-Child-FINAL.pdf>.
- Medietilsynet, Robust, resigned or numb? – Interviews with young people and parents about harmful content online, 2024, https://www.medietilsynet.no/globalassets/dokumenter/rapporter/240205_robust_resignert_nummen.pdf.
- Memon, A. M., Sharma, S. G., Mohite, S. S., & Jain, S. (2018). The role of online social networking on deliberate self-harm and suicidality in adolescents: A systematized review of literature. *Indian journal of psychiatry*, 60(4), 384-392.
- OECD, Towards Digital Safety By Design For Children, OECD Digital Economy Papers, June 2024, No. 363, https://www.oecd.org/en/publications/towards-digital-safety-by-design-for-children_c167b650-en.html.
- Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., and Hasebrink, U. (2020). EU Kids Online 2020: Survey results from 19 countries. *EU Kids Online*. <https://doi.org/10.21953/lse.47fdeqj01ofo>.
- Staksrud, E. & Livingstone, S. (2009). Children and online risk: Powerless victims or resourceful participants? *Information, Communication and Society*, 12(3): 364–387. <http://eprints.lse.ac.uk/30122/>






Stem4. (2022). Body image among young people: Negative perceptions and damaging content on social media, combined with pandemic fallout, contribute to a low sense of self-worth and a rise in eating difficulties, new survey reveals, <https://stem4.org.uk/wpcontent/uploads/2022/12/Body-image-among-young-people-Negative-perceptions-anddamaging-content-on-social-media...-new-survey-reveals-Dec-22.pdf>.

Wood, S. (2024). Children and Social Media Recommender Systems: How Can Risks and Harms be Effectively Assessed in a Regulatory Context?. Available at SSRN 4978809.



Avenue Louise 475 (box 10)
1050 Brussels, Belgium
+32 2 230 83 60
info@cerre.eu
www.cerre.eu

-  Centre on Regulation in Europe (CERRE)
-  CERRE Think Tank
-  CERRE Think Tank

