cerre Centre on Regulation in Europe

DSA IMPLEMENTATION FORUM

FUTURE OF THE DSA: SAFEGUARDING MINORS IN THE DIGITAL AGE

March 2025

Miriam Buiten
Michèle Ledger
Christoph Busch

cerre

DSA Implementation Forum

Future of the DSA: Safeguarding Minors in the Digital Age

Miriam Buiten
Michèle Ledger
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.

info@cerre.eu – www.cerre.eu

Table of Contents

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, digital industry, and service sectors. 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.

Michèle Ledger is a researcher at the CRIDS research centre of the University of Namur where she also lectures on the regulatory aspects of online platforms at the postmaster degree course (DTIC). She has been working for more than 20 years at Cullen International and leads the company's Media regulatory intelligence service.

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.

Executive Summary

The 2024 edition of the DSA Forum focuses on the protection of minors. This focus reflects both the widespread attention to the issue and the critical importance of ensuring children's safety in digital environments. Among the many challenges of protecting minors online, two issues stand out as particularly pressing: age assurance and age-appropriate design. These interconnected topics raise important questions about the balance between protecting children online and preserving their rights to access digital information and opportunities.

The EU's Digital Services Act (DSA) introduces tailored due-diligence obligations on online intermediaries to foster a safer online environment, while also respecting fundamental freedoms such as freedom of expression. Online platforms are also required under the DSA to protect minors and very large online platforms, and search engines are subject to additional risk mitigation measures, in particular for risks posed to children. These rules are open ended and are principle-based which is why the European Commission is adopting guidance.

The issue paper on **Age Assurance** explores the ecosystem of EU provisions linked to age assurance alongside key initiatives relating to age assurance in some of the EU Member States, in the UK and in Australia. It highlights that **the DSA does not mandate age assurance at the EU level**, nor does it define the type of content that should not be accessed by minors, and it does not set a minimal age for accessing (certain types of) online services or content. In the meantime, **some Member States have recently adopted legislation which mandates age assurance (and age verification) to prevent minors from accessing online pornography and in some cases other types of particularly harmful content.** This is creating internal market fragmentation which has been brought to the attention of the Member States concerned under the EU's 'Regulatory Transparency' procedure.

While the paper does not examine the detail of the technical assurance systems and does not take position on whether age assurance should be mandated, it **does call for the guidelines to address this issue and to seek to put an end to the national fragmentation which is jeopardising the functioning of the internal market**.

Also, from the comparative analysis of the regulatory framework, it the **guidelines may not be sufficient,** and a **targeted legislative initiative may be needed** to oblige online platforms to put in place age verification to prevent minors from accessing **online pornography platforms** (and possibly other particularly harmful types of content). The EU level framework should **also address the level of oversight (if any and by who?) of the technology to be used**.

Other clarifications are also needed such as on the **interplay between the DSA and the Audiovisual Media Services Directive** (AVMSD) which allows Member States to enact further rules to protect minors when they use video sharing platforms. In any event, age assurance technology should not be mandated without clear justification given the important trade-offs for the **minors** (who will be deprived from accessing certain content), for **adult users** (who will need to accept that a certain amount of personal data is collected) and for the **platforms** themselves (who will need to adapt and deploy the systems). **These systems should not be used lightly but should be clearly grounded and deployed in a proportionate manner.**

The issue paper **Age-Appropriate Design** examines the goals of age-appropriate design within the context of the DSA's child safety obligations. Given the broad formulation of these obligations, the paper emphasizes the critical role of the Commission's guidance in clarifying the specific measures platforms must implement to uphold the DSA's obligation to **ensure a high level of privacy, safety, and security for minors**.

Considering both **specific design measures** and **broader governance mechanisms** that platforms can adopt to protect children, the paper identifies **guiding principles** for ensuring children's online safety. It advocates for a framework that is both adaptable and concrete, categorizing **best practices, grey areas and high-risk practices that should be outright prohibited.** Additionally, the paper presents concrete example scenarios across different service aspects – such as default settings and recommender systems – offering practical insights that could inform the Commission's guidelines and help platforms operationalize the DSA obligations effectively.

In relation to the Commission's forthcoming guidelines, the paper emphasizes the need for:

- **Clear and actionable guidance** that clearly distinguishes between the binding obligations under the DSA and additional recommendations;
- **A risk-based enforcement approach** that balances risks and benefits, ensuring a comprehensive assessment of the overall impact on children's safety and well-being;
- **A labelling or certification system** (such as a "Child-Safe Certified" designation) that could act as a visible marker, signalling that a platform has met rigorous, clearly defined standards for child protection.

The Issue Paper **Charting the Path for Protection of Minors Under the DSA sheds light on the interlinkages aga assurance and age-appropriate design** in the sense that age assurance alone is not a silver bullet for ensuring online safety for minors. Instead, it must work in tandem with thoughtful, child-centric design.

Clear links between the two topics should therefore be made in the enforcement of the DSA.

The paper highlights the complexity of the regulatory landscape and that some services are not covered by EU legislation. The enforcement of the rules will require a high level of coordination given that multiple of oversight bodies are potentially in charge: the European Commission for the rules applicable to VLOPS and VLOSEs; digital service coordinators; national data protection authorities; national competent authorities in relation to consumer protection; and media regulatory authorities.

Lastly, the paper puts forward the idea that the Commissions guidelines could be conceived as a 'living document', open to regular updates to reflect emerging risks, emerging technology developments and best practices.

Issue Paper

Charting the Path for the Protection of Minors under the DSA

Miriam Buiten
Michèle Ledger

March 2025

1. Charting the Path for Protecting Minors under the DSA

The 2024 edition of the DSA Forum focuses on the protection of minors. This focus reflects both the widespread attention to the issue and the critical importance of ensuring children's safety in digital environments. Among the many challenges of protecting minors online, two issues stand out as particularly pressing: **age assurance** and **age-appropriate design**. These interconnected topics raise important questions about the balance between protecting children online and preserving their rights to access digital information and opportunities.

The Issue Papers presented in this Forum are not meant to present definitive solutions or take strong positions. Instead, they aim to illuminate the areas where deeper discussion and debate are needed. For instance, to what extent should detailed regulatory obligations shape the online protection of minors? How do we weigh the need to minimise risks against children's rights to explore the opportunities of the digital world? These are not merely technical questions but deeply political ones, requiring clear decisions about roles, responsibilities, and regulatory approaches.

The need for regulatory oversight has become increasingly apparent in recent years. Experience has shown that relying only on platforms to self-regulate is insufficient. While the DSA establishes a foundational framework, the specific rules on the protection of minors are open-ended, offering few specifics about what platforms must do to comply. Even the term "minors" is mentioned sparingly in the DSA, leaving critical aspects of their protection to interpretation. Although the DSA sets obligations for safe design and risk minimization, it provides little concrete guidance on what these mean in practice. This framework of broad but open-ended rules creates a **need for a clear framework for clarifying obligations and assigning responsibilities**.

This highlights the need for the forthcoming **guidance from the European Commission on the protection of minors**. The stakes are high: this guidance could define the future of online safety for children, establish best practices, and potentially also address how to deal with the gaps and ambiguities in the current regulatory framework. It is essential to clarify the purpose of this guidance must clarify its purpose. Will it act as a guide to interpreting the DSA's enforcement obligations, or will it go further and offer a set of non-binding recommendations—a 'nice-to-have' roadmap for platforms? This distinction will play an important role in shaping the regulatory landscape.

Central questions include: What specific measures are needed for age assurance to address the internal market problem? Can age-appropriate design frameworks go beyond aspirational principles to drive meaningful, enforceable change? Without clear answers, platforms and regulators alike will struggle to create environments where children are well-protected.

The Issue Papers part of this DSA Forum seek to highlight these questions and point out issues that need thoughtful deliberation and decisive action. The papers seek to put forward a few building blocks to arrive at a coherent framework that that not only safeguards children while empowering them to thrive in the digital age, but that also allows digital services to be deployed in the EU on a cross-border basis.

1.1 DSA Obligations

Most of the rules of the DSA that protect minors apply to online platforms and to very large online platforms (VLOPs)and very large online search engines (VLOSEs). **Article 28 DSA** is one of the core rules as it specifies that all **online platforms** (such as social media, video-sharing platforms, app stores and marketplaces) that are accessible to minors must take appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors. The Commission is set to issue guidelines on this article.

Articles 34 and 35 oblige **online platforms (and search engines) designated by the Commission as very large** (active monthly EU users above 45 million) to annually assess negative effects of their services for the protection of minors, the rights of the child, and serious negative consequences for their physical and mental well-being and mitigate any identified systemic risk.

Article 14 DSA obliges **all intermediaries** to **specify any restrictions they impose in relation to the use of their service** in respect of information provided by the recipients of the service, in their terms and conditions (T&C). **They should also act in a diligent, objective and proportionate manner in applying and enforcing T&C with due regard to the rights and legitimate interests of all parties involved**, including the fundamental rights of the recipients of the service. Where an intermediary service is primarily directed at minors or is predominantly used by them, the provider of that intermediary service needs to explain the conditions for, and any restrictions on, the use of the service in a way that minors can understand.

The DSA is also part of a pre-existing ecosystem of EU norms at the EU level. In particular, the Audiovisual Media Services Directive (AVMSD) contains a set of minimum rules to protect minors from harmful content when they are exposed to **audiovisual services on linear television, on-demand and video sharing platforms (VSPs)** such as YouTube. Other rules also exist which are further exposed in the respective Issue Papers.

2. Common Themes

2.1 Interaction between Age Assurance and Age-appropriate Design

The Issue Papers on age assurance and age-appropriate design highlight several key themes. These two approaches are interconnected—**age assurance alone is not a silver bullet for ensuring online safety for minors. Instead, it must work in tandem with thoughtful, child-centric design**.

Age assurance is not just about granting or restricting access to a platform or to age-rated content—it is a central component of age-appropriate design. Once a platform identifies a user as a minor, it must adapt its design accordingly. This means not only determining what content is served to them based on their age but also how it is presented—through curation, recommendations, and engagement mechanisms.

A fundamental challenge is making these principles operational in practice. A user's age is essential for deciding whether they can access a platform, what content they should be exposed to, and how they are treated within the service. There is a need to develop a framework here, but implementing such a framework raises various questions. For instance, one could consider that:

- On some platforms (e.g. adult content sites), no child-safe content exists, so access should be entirely blocked for minors;
- On others, all content is child-friendly, making access is straightforward;
- The most difficult cases lie in between—such as social media platforms where user-generated content (UGC) may include material particularly harmful to minors. These platforms could allow minors but should ensure that content shown and the way in which it is shown, as well as other design features, are adapted for minors. This raises legal challenges: how can platforms be required to protect minors without indirectly mandating general content monitoring?[1]

A key challenge is determining who should decide — and how — what content and design adjustments are necessary to protect minors. Once a platform verifies a user's age and identifies the need to shield them from certain content or design features, the question becomes: what exactly qualifies as problematic? Since the DSA does not itself define illegal or harmful content, leaving that to national laws and sector-specific EU regulations, there remains significant room for interpretation regarding the content and design elements platforms must address for underage users under Arts. 28, 34 and 35 DSA.

Guidelines can help clarify expectations, but there are inherent limits. The DSA focuses on procedural obligations rather than setting substantive rules on content. It requires platforms to mitigate risks through content moderation and design measures without clearly defining what these measures should entail, particularly when it comes to harmful but legal content. This creates a fundamental tension: platforms are required to apply age-appropriate measures, yet there is little concrete

[1] DSA Art. 8

guidance on what content or design is actually harmful or unsuitable for minors. In practice, identifying risks to be mitigated—as the DSA requires—inevitably involves making judgments about what is harmful to minors. While the DSA outlines risks in broad, principle-based terms, platforms are left to determine, in practice, where to draw the line.

If the guidelines are to serve as a rulebook for enforcement—clarifying when age verification or assurance is appropriate and which design measures are needed to mitigate risks for minors—then clear guidance linking age verification and age-appropriate design is also essential. Once a platform knows a user's age and the necessary design measures for minors have been identified, it must be clear which measures apply in which scenarios. In other words, under what specific circumstances should a platform take particular actions to protect minors? While the DSA emphasises risks related to safety, security, and privacy, making these principles operational requires translating them into concrete actions—defining how they apply to content moderation, platform practices, algorithmic recommendations, user settings, and other design elements.

At the same time, these **guidelines must remain flexible enough** to accommodate the diverse range of online services and content, avoiding overly rigid rules. Striking the right balance in implementing these measures is not always straightforward, and it must be debated who will take such decisions.

As noted above, age assurance is a key element of age-appropriate design, and the two could become increasingly intertwined in terms of enforcement. To mitigate risks effectively, regulators could even consider a **system of escalating requirements**—not foreseen by the DSA itself, but as a potential future approach to enforcement. Under such a system, if a platform fails to implement effective design protections for minors, it could be required to apply stricter age assurance measures to prevent minors from accessing the platform altogether. An alternative scenario could be that in the absence of specific age appropriate design features for minors, by default all content should be safe for all users (if the platforms does not restrict access to minors through age verification in the first place). This solution is enshrined in the Dutch Media Law to protection minors from harmful content on audiovisual media services.[2]

These approaches reflect an implicit link: if platforms do not adequately safeguard minors once they are online, they may need to take stronger steps to block access entirely. However, determining the precise conditions under which such measures would apply—and establishing clear enforcement criteria—remains a significant challenge.

Moving forward, **regulators must consider how to integrate age assurance and age-appropriate design in a practical and meaningful way**. This requires concrete guidelines on when and how platforms should implement protections, ensuring that safety, security, and privacy risks are addressed through clear, enforceable standards.

2.2 Overall Coherence of the Regulatory Framework

The regulatory landscape is complex because the **rules on the protection of minors of the DSA are intertwined with other rules** - which are either sector specific like those contained in the Audiovisual

[2] Art. 4.1 of the Dutch Media Law

Media Services Directive (AVMSD)[3] or horizontal such as those contained in the GDPR or in consumer protection legislation. The articulation between these rules is not necessarily simple and may lead to oversight issues in particular (see below).

There **may also be potential gaps** in the services covered under the DSA and the AVMSD. Indeed, certain high-risk services fall outside the scope of these instruments, such as pornographic websites without user-generated content. Given their distinct potential risks, these platforms may require a tailored approach, similar to the UK's Online Safety Act, which imposes specific risk assessments obligations.

The potential gaps in the EU legislative framework are problematic not only because some member states are trying to address them (which is creating internal market frictions, see below) but also because, ultimately minors should be protected irrespective on the type of online service they use. This raises the broader question of whether the EU should consider introducing rules to protect minors that are not dependent on the type of platforms, i.e. all digital services would be covered in the same way. The guidelines will probably not be able to settle all these questions. They could however flesh out interactions between the frameworks including on their enforcement.

2.3 Internal Market Fragmentation

The work highlights a **high risk of internal market fragmentation on the issue of age assurance and age verification in particular**. This stems from the fact that Member States are particularly concerned about making sure that minors do not access online pornography (and other specific types of particularly harmful content) and are hence imposing obligations on non-national established digital services, sometimes irrespective of their qualification as an online platform. Such a threat in relation to rules on appropriate design does not yet exist, but if the EU does not clarify what is expected from platforms and from regulators (in their enforcement action), some Member States may also decide to enact national rules.

It is therefore urgent for the European Commission to put an end to these national rules and to develop sufficiently robust rules at the EU level so that minors are fully protected, while also allowing cross-border digital services to flourish in the EU.

2.4 Ecosystem of oversight bodies

As the Issue Papers show, the rules on the protection of minors contained in the DSA are intertwined with other rules that are scattered between different pieces of legislation. Multiple authorities may therefore have an enforcement mandate: the European Commission for the rules applicable to VLOPS and VLOSEs; digital service coordinators; national data protection authorities; national competent authorities in relation to consumer protection; and media regulatory authorities. A major challenge will be to **ensure a consistent and effective oversight and enforcement of the rules on the protection of minors**.[4] This will require careful coordination to address the evolving challenges.

[3] The AVMSD contains a set of minimum rules to protect minors from harmful content when they are exposed to audiovisual services on linear television, on-demand and video sharing platforms (VSPs) such as YouTube

[4] G. Monti and A. de Streel, *Improving institutional design to better supervise digital platforms*, CERRE Report, January 2022.

In any event, the work of the European Board for Digital Services (EBDS) will be central to ensure coordination in the enforcement of the DSA. We urge the EBDS to ensure proper cooperation with the recently launched European Board for Media Services (EBMS) since both sets of national authorities (digital service coordinators for the former and the media regulators for the later) will be at the forefront of enforcement actions (unless the European Commission takes the lead in relation to VLOPs and VLOSEs).

Also, because of the open-ended nature of the rules on the protection of minors contained in the DSA, **regulators will probably need to be in constant dialogue with the platforms**. The guidelines could therefore also address the need for a regular dialogue between platforms and competent authorities.

3. Outlook

The Commission's forthcoming guidelines on the enforcement of Article 28 DSA will be central in providing clarity for platforms, outlining what is expected of them in practice. These guidelines will offer much-needed guidance on two closely linked issues highlighted in this first edition of the DSA Forum: age assurance and age-appropriate design. By translating the DSA's general obligations into more concrete and actionable requirements, the guidelines will help platforms understand how to align their systems, processes, and design choices with regulatory expectations. This clarification is particularly important given the procedural focus of the DSA, which leaves significant room for interpretation when it comes to practical implementation—especially in areas such as protecting minors from harmful but legal content and ensuring platform design is appropriate for younger users.

The positive outcomes we can expect from the guidelines are several. *First*, the guidelines should provide **concrete measures for risk mitigation**. They can be expected to specify the actions platforms must take to mitigate risks. In relation to minor protection, this includes clarifying how platforms will be required to adapt content moderation practices and redesign platform features to better safeguard minors, thereby offering clearer expectations on how platforms should meet regulatory standards.

Second, the guidelines are likely to provide **clarity on age assurance as a key component of age-appropriate design**. They are expected to strike a balance between restricting access for minors through effective and practical age-assurance measures, while also refining content moderation and design features for users already on the platform. This balance is critical for creating a safer online environment for minors, enabling both proactive access controls and reactive content management, thereby allowing minors to access online spaces and content securely.

In a broader sense, the guidelines will help **set standards for platform accountability**. By establishing clear benchmarks for compliance, the guidelines will identify specific standards platforms must meet, such as what constitutes 'appropriate design' and 'age-appropriate content.' This will offer a clearer regulatory framework that platforms can follow to protect young users effectively.

The guidelines could be conceived as a **'living document'**, meaning they would remain open to regular updates to reflect emerging risks, evolving technological developments, and new best practices. Given the fast-paced nature of the online environment, where platform design, business models, and technological capabilities are constantly evolving, static guidance would quickly become outdated and risk losing its relevance and effectiveness. By adopting a living document approach, the guidelines could continuously incorporate insights from enforcement practice, research, and stakeholder input—including from civil society, child protection experts, industry, and regulatory authorities. This would ensure that platforms have access to up-to-date, practical guidance.

Such a dynamic approach would also help align the guidelines with emerging regulatory and legislative initiatives, ensuring they remain coherent within the broader EU digital rulebook. Ultimately, this flexibility would allow the guidelines to stay ahead of the curve, promoting innovation in the service of minors' safety and helping to shape a digital environment that keeps pace with technological change—while maintaining a strong focus on child protection and rights.

Despite the positive outcomes that could stem from the guidelines, the Issue Papers also highlight that targeted legislative initiatives could potentially still be necessary. While the guidelines will provide

much-needed clarity, they cannot address all gaps in EU legislation concerning the services within scope. For instance, the guidelines may suggest that the most harmful types of content for minors should not be accessible to them, but this may not resolve the national fragmentation discussed in the Issue Paper on age assurance. Likewise, the guidelines will probably be unable to address the interaction between the DSA's rules on the protection of minors and those outlined in the AVMSD for VSPs.

Given the open-ended nature of the DSA's provisions on minor protection, **effective oversight of how these rules are applied will be essential**. This oversight will require a **robust dialogue** between platforms and the competent authorities, ensuring that implementation is consistent, transparent, and adaptable to evolving online risks. Ongoing collaboration and communication between regulators and platforms will be vital to making the guidelines and their enforcement effective.

Issue Paper

Protection of Minors: Age Assurance

Michèle Ledger

March 2025

1. Introduction

According to a study conducted by the French regulator, ARCOM, 2.3 million minors visit pornographic websites every month. This number has been growing rapidly in recent years and is correlated with the democratisation of mobile terminals among children. The proportion of minors visiting 'adult' sites has risen by 9 points in 5 years, from 19% at the end of 2017 to 28% at the end of 2022. Every month in 2022, more than half of boys aged 12 and over visited such sites, a percentage that rises to two-thirds for boys aged 16 and 17. On average, 12% of the audience on adult sites is made up of minors"[5].

Next to pornography content, there is also evidence that certain types of content pose a special risk for the development of children such as cyberbullying, sexual harassment, violence, and content that advocates dangerous or unhealthy or dangerous behaviours, such as self-harm, suicide and anorexia.[6]

In the European Union, according to a report from the European Audiovisual Observatory,[7] access control measures are generally absent from some of the large Video-Sharing Platforms (VSPs) which tend to rely on self-declaration of users during the sign-up phase. The report also flags « an evident lack of initiative from most pornography providers to implement measures that prevent children from accessing their services and being exposed to their content ». It is true that the Audiovisual Media Services Directive that was revised in 2018 (and which introduced rules for VSPs) was finally transposed in all the Member States very late.[8]

Making sure that minors do not access harmful services and content that could impair their development has become in recent years a major concern for policy makers at the EU level, in some of the Member States and in other jurisdictions around the world.

The EU Digital Services Act[9] (DSA) has introduced several rules on the protection of minors and the enforcement of these measures has become one of the enforcement priorities of the European Commission in relation to the Very Large Online Platforms it supervises. These rules also need to be enforced by the national competent authorities designated as such by the Digital Service Coordinators (DSCs).

Despite the fact that the DSA introduces fully harmonised rules on the protection of minors for the platforms in scope, some Member States are moving towards the adoption of rules to oblige websites

[5] Translated with DeepL.com (free version), source : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000050385836. The study was based on data supplied by Médiamétrie.
[6] The OECD also identifies that risks online for minors that are not only related to content, but more broadly to contract, conduct and contract (OECD 4Cs framework), available at https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5df252f14&appId=PPGMS
[7] The protection of minors on VSPs: age verification and parental control, European Audiovisual Observatory, Strasbourg, 2023
[8] Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities.
[9] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) OJ L 277, 27.10.2022, p. 1–102

to assess the age of users, either at the sign-up stage or when users wish to access content that is age restricted.

The Issue Paper:

- Explains **the ecosystem of EU provisions** that are directly or indirectly linked to **age assurance**;
- identifies some of **the Member States' initiatives on age assurance and their effects on the functioning of the internal market;**
- brings to light some recent initiatives from countries outside of the EU, namely Australia and the UK.

The paper does not examine the detail of the technical solutions for age assurance, nor does it take position on whether age assurance (age verification or age estimation) should be mandated.

Indeed, putting in place age assurance, and age verification in particular, carries important trade-offs, for **minors** (who may deprived from accessing some content) **for adult users** (who will need to accept that a certain amount of personal data is collected) and for the **platforms** themselves (who will need to adapt and deploy the systems).[10] These systems should not be deployed lightly, but should be clearly grounded and deployed in a proportionate manner.

The Issue Paper seeks to shed light on the current situation and to make recommendations on the areas where EU policy makers need to make decisions to arrive at a coherent set of rules at the EU level. Indeed, EU-wide harmonisation is desirable because the current fragmentation of national rules appears both detrimental to the protection of minors and to the deployment of pan-European digital services.

In this paper, we refer to **age assurance** as an umbrella term that covers methods used to determine an individual's age (or age range) with different levels of confidence or certainty.[11] Self-declaration traditionally forms part of age assurance but it is widely recognised that this is not a reliable method since it can easily be circumvented. The report therefore focuses on:

Age verification which is "a system that generally relies on hard (physical) identifiers and/or verified sources of identification, to determine the individual's age or age-range, to a specified level of confidence, to provide a higher degree of certainty in determining the age or age-range of an individual than age estimation techniques".

Age estimation which generally relies on estimation by reference to inherent features or behaviours related to the individual, to determine that the individual's age is likely to fall within an age-range, to a specified level of confidence, to provide a lower degree of certainty in determining the age or age-range of an individual than age verification techniques.[12]

[10] Age Assurance, Guiding Principles and Best Practices, Digital Trust & Safety Partnership, September 2023, p.2
[11] These definitions are in euCONSENT.. D5.1 Common Vocabulary. https://euconsent.eu/project-deliverables/#

[12] Livingstone, S., Nair, A., Stoilova, M., van der Hof, S., & Caglar, C. (2024). Children's Rights and Online Age Assurance Systems: The Way Forward. *The International Journal of Children's Rights*, *32*(3), 721-747. https://doi.org/10.1163/15718182-32030001

These systems can be deployed to prevent minors from accessing certain services or certain content but also to provide children with appropriate experience depending on their (evolving) capacities.

2. Ecosystem of Norms at the EU level

2.1 Age Assurance is Not Mandated

There are multiple norms at the EU level that point towards the need to prevent minors from accessing harmful content on the internet. However, none of these EU rules go as far as to define the type of content that should not be accessed by minors, they do not set a minimal age for accessing (certain types of) online services or content and they do not mandate age assurance. The EU wide norms have been put in place progressively over the years and the result is **an ecosystem of rules that are lacking clarity and coherence.** Some Member States are therefore filling the gaps, each in their own way, which is jeopardising the functioning of the internal market (see 3).

The EU level rules are listed in a Compendium of EU formal texts concerning children in the digital world, elaborated under the New Better Internet for Kids Strategy (BIK+).[13] In relation to preventing minors from accessing certain content, the ecosystem of rules consists of two main legislative instruments: the Digital Services Act and the Audiovisual Media Services Directive, but other EU norms and initiatives also exist.

2.2 The Digital Services Act and the Audiovisual Media Services Directive

Historically, the first set of rules that obliged service providers to protect minors was contained in the Audiovisual Services Directive.[14] The rules apply to linear and non-linear audiovisual services, over which providers have editorial control. Since 2018, rules also apply to Video Sharing Platforms.

According to Article 28b AVMSD, VSPs need to put in place "appropriate measures" to protect minors from content that could impair their physical, mental or moral development. **Age verification** is mentioned in the AVMSD as a possible way to ensure that minors do not have access to harmful content, but it is not mandated.

The DSA also contains rules that relate to the protection of minors and to age assurance/verification:

- Article 14 DSA obliges all intermediaries to specify any restrictions they impose in relation to the use of their service in respect of information provided by the recipients of the service, in their terms and conditions (T&C). They should also act in a diligent, objective and proportionate manner in applying and enforcing T&C with due regard to the rights and legitimate interests of all parties involved, including the fundamental rights of the recipients of the service. Where an intermediary service is primarily directed at minors or is predominantly used by them, the provider of that intermediary service shall explain the conditions for, and any restrictions on, the use of the service in a way that minors can understand. In short, all intermediaries should be transparent in restrictions of use in their T&C and make sure to apply the rules they set for themselves.

[13] Available at https://op.europa.eu/en/publication-detail/-/publication/8e18982d-0db6-11ef-a251-01aa75ed71a1/language-en
[14] Directive (EU) 2010/13 concerning the provision of audiovisual media services as amended by Directive 2018/1808

- Article 28 DSA is one of the core rules as it specifies that online platforms (such as social media, video-sharing platforms, app stores and marketplaces) that are accessible to minors must take appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors. The Commission is set to issue guidelines on this article.
- Articles 34 and 35 whereby the online platforms (and search engines) designated by the Commission as very large (active monthly EU users above 45m) must annually assess negative effects of their services for the protection of minors, the rights of the child, and serious negative consequences for their physical and mental well-being, and mitigate any identified systemic risk. The list of possible mitigation measures they need to deploy includes age verification.

These norms have been analysed as implying a risk-based approach[15] which implies a tailored responses according in particular to the to the type of content available and the type of service.

2.3 Other EU-level Norms and Initiatives

GDPR

Article 8 of the General Data Protection Regulation (GDPR) provides that when data processing is based on consent and when online services are directly offered to children, the processing is lawful where the child is at least 16 years old. If the child is below 16 years, consent should be given or authorised by the holder of parental responsibility. However, the member states may set a lower age for when children can begin to give consent, as long as it is not below the age of 13.[16] This provision implies that online services that are offered to children should check the age of their users to make sure they are not under the age of consent for GDPR purposes. Also when age assurance is deployed, the rules of the GDPR will come into play regarding the data processing that is done by such mechanisms. This is not covered by this paper but has recently been addressed by the European Data Protection Board.[17]

The Rights of the Child

A key aspect of the discussion on age assurance is the need to take into consideration the rights of the child. Article 24 of the Charter of Fundamental Rights in the European Union enshrines the rights of the child and in particular, the right to be protected and the right to express views freely. The European declaration on Digital Rights and Principles for the Digital Decade contains a special title on the 'Protection and Empowerment of Children and Young People in the digital environment'. This non-binding but influential text highlights the need to (in relation to children and young people) promote positive experiences in an age-appropriate and safe digital environment; to provide opportunities to all to acquire the necessary skills and competences, including media literacy and critical thinking, in order to navigate and engage in the digital environment actively, safely and to make informed choices.

[15] Livingstone et al (2024), p. 6
[16] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation
[17] Statement 1/2025 on Age Assurance, 11 February 2025, available at https://www.edpb.europa.eu/system/files/2025-02/edpb_statement_20250211ageassurance_en.pdf

Children and young people also need to be protected against harmful and illegal content, exploitation, manipulation and abuse online.

At the international level, the United Nations Convention on the rights of the child in relation to the digital environment states that "states parties should ensure that children have access to information in the digital environment and that the exercise of that right is restricted only when it is provided by law and is necessary for the purposes stipulated in Article 13 of the Convention" and that "any restrictions on children's right to freedom of expression in the digital environment, such as filters, including safety measures, should be **lawful, necessary and proportionate**". According to Article 13 restrictions are only allowed if they are provided by **law** and if they are necessary for the respect of the rights or reputations of others for the protection of national security or of public order, or of public health or morals.[18]

The European Digital Identity Framework (EUdi) Regulation

Article 5 (f) of the European Digital Identity Framework (EUdi) Regulation requires very large online platforms (VLOPs, but not very large online search engines) designated under the DSA to accept and facilitate the use of the European Digital Identity Wallet as a method for user authentication.[19] In so doing, VLOPs need to respect the principle of data minimisation, meaning that they will only be able to require the necessary personal information for accessing the service. Further, according to the regulation, users are under no obligation to use the wallet to access the services and their access should not be hindered because they decide not to use the wallet.

Proposed CSAM regulation

A proposed regulation on the detection, reporting and removal of child sexual abuse material (CSAM) is in the course of adoption. While the proposal is aimed at providing a long term legal solution to enable the detection of CSAM in interpersonal communications services, it also targets hosting services (such as social media platforms and cloud services).

Providers would have to conduct regular risk assessments to assess the risk of dissemination of CSAM on their services and take mitigating measures. For instance, these risk assessments need to take into account functionalities enabling age-verification.

According to the Commission's initial proposal, app stores would need to verify the age of users that want to access apps that carry a risk of grooming. The Parliament has proposed to only oblige app stores designated as gatekeepers under the Digital Market Act to take certain measures to protect children in relation to apps that based on their information should not be accessed by children.

The Council had at the time of writing still not adopted its negotiating position on the text.

[18] Available at https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child. See also general comment N° 25 on the rights of the child in the digital environment, https://www.right-to-education.org/sites/right-to-education.org/files/resource-attachments/UN_CRC_General%20comment%20No.%2025%20%282021%29%20on%20children's%20rights%20in%20relation%20to%20the%20digital%20environment_En.pdf

[19] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework

Better Internet for Kids Strategy (BIK+)

The Commission's Communication of 2022 on "a digital decade for children and youth: the new European strategy for a better internet" (BIK+) aims to ensure that children are protected and empowered in the new digital decade. In this document, the Commission announced that it will facilitate an EU code for age-appropriate design and requested a European standard on online age verification to be set up by 2024.[20]

Towards a Universal Age Verification Solution in the EU?

The European Commission published on 14 October 2024 a **call for tender to develop a « universal age verification solution »** to allow users to access an age-restricted online service by verifying their age, without requiring the sharing of added personal data. This solution could be used by social media platforms, gambling platforms or adult platforms. The call is specifically addressed to access the online services that are restricted to 18+, even if the solution should allow for age-appropriate access whatever the age restriction. The solution will be rolled out under the EUdi wallet.[21] The Commission's overall aim with this procurement is to «seek a Europe-wide effective and convenient method to age-gate access to specific online services».

[20] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:212:FIN, see annual review for 2024 here: https://better-internet-for-kids.europa.eu/sites/default/files/2025-02/BIK_Report2024_WEB_0.pdf

[21] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/tender-details/docs/ae950883-112f-4139-989e-1c8d794bb77a-CN/EN_TENDER_SPECIFICATIONS_EC-CNECTLUX2024OP0073_Age%20verification%20solution_Part2_finalised_20241011_V1.pdf

3. Ecosystem of Rules in EU Member States

This section reviews national initiatives on age assurance in some of the Member States.[22] Some of these initiatives derive from the transposition of Article 28b AVMSD on the protection of minors in relation to VSPs, while others target a wide range of services, and are potentially raising internal market concerns. The analysis of these national developments is useful on two accounts:

- First it shows why and how the member states are addressing age assurance
- Second it will shed light on the aspects that are challenged by the European Commission (see Section 4)

3.1 France

France adopted a law to secure and regulate the digital space ("Loi Sren") on 21 May 2024.[23] The law requires the regulator (Arcom) to establish binding technical requirements ("référentiel") for age verification systems to be met by websites **that make available pornographic content** (Streaming/Video on demand services are also covered).

The standards were adopted on 8 October 2024. They require operators of porn services to refrain by default from displaying pornographic content until they have verified that the user is **at least 18** (either by blurring the home page or by using another mechanism such as the Restricted to Adults (RTA) label. Some of the other measures they need to take include:

- make available an age verification system that complies "with double anonymity" privacy protection standards;
- distinguish with certainty minors from adults and prevent circumvention (such as preventing the sharing of the proof of age with other people and avoiding the risks of attacks such as deepfakes, spoofing, etc.);
- avoid discrimination (e.g. the effectiveness of the age verification solution must be the same whatever the physical characteristics of the user);
- ensure that verification is carried out each time the service is consulted, without requiring the creation of a user account.

Arcom's référentiel also contains detailed requirements on the need to respect personal data standards.

The SREN law foresees that Arcom can request service providers to carry out audits of their age verification systems to assess them against the technical standards it established. These audits need to be carried out by independent organisations.

[22] This account is partially based on Cullen International's Benchmark on Protection of minors : overview of initiatives on age-verification systems in European Countries, https://www.cullen-international.com/client/site/documents/CTMEEU20240056 (updated November 2024)
[23] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000049563368

The Law contains detailed rules on sanctions. In case of non-compliance with the formal notice to use age verification, Arcom can impose a financial penalty up to 3% of the provider's worldwide turnover, whichever is higher (and 5% of turnover in case of repeated non-compliance). Arcom is also empowered to request **Internet access service providers or domain name systems to block the URL addresses on non-compliant service providers**. **Search engines can also be ordered to delist services**. Fines are foreseen against intermediaries who do not prevent access.

Separately, France adopted a law to establish a digital age of majority and combat online hate on 7 July 2023.[24] It foresees that users must be at least 15 to register on social media platforms, unless their parents or holders of parental responsibility have given their consent. The law also specifies that social media platforms need to use technical verification systems as specified by Arcom's référentiel. The rules were set to apply to social media platforms that exercise their activity in France. The law has not been put into application, in view of its incompatibility with EU legislation (see below).

3.2 Ireland

The Online Safety Code of 21 October 2024 applies to **VSPs** and gives effect to Article 28b AVMSD.[25] It aims in particular at protecting children from **pornography and extreme or gratuitous violence**. It requires VSPs that allow this type of content to use an "effective" method of "age assurance" to that "children" do not normally encounter this content. **Platforms will also need to use appropriate forms of age verification, depending on their size and nature, to protect children from video and associated content which may impair their physical, mental or moral development. For this purpose, this includes effective age assurance measures including age estimation.**

Children means a person under the **age of 18**. An effective age assurance cannot be based solely on self-declaration of age, but standards for effective age assurance are not specified in the code.

It is interesting to note that these rules only apply to the extent that the VSP's terms and conditions of use do not preclude the uploading/sharing of adult only video content. Next to the need to put in place effective age assurance, the VSPs also need to establish an easy-to-use content rating system to allow users to rate content as not suitable for children because the video content is adult-only and to tag the video content accordingly to ensure transparency for users that view the content.

Another interesting feature of the Irish system is that the systems that need to be deployed by VSPs to deal with complaints need to also address possible issues in relation to age assurance.

3.3 Italy

Law 159 of 13 November 2023[26] requires **website operators and VSPs** (including streaming/VOD services) that disseminate **pornographic images and videos** in Italy to verify that users are **above the age of 18.**

The law tasks the regulator, AGCOM, with defining the procedural/technical measures. AGCOM announced the adoption of these measures on 7 October 2024. In a nutshell, website operators and

[24] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047799533
[25] As transposed in section 139K of the Online Safety and Media Regulation Act.
[26] https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2023-11-13;159!vig=2024-02-12

providers of video-sharing platforms, that disseminate pornographic images and videos in Italy, must communicate to the Authority the third parties entrusted with the age verification operation (the independent third party), together with a report containing any useful information on the entity; on the method of age verification and on the reasons for the choice, for the purposes of the supervisory activity under their responsibility. The age assurance system must

- be certified and be legally and technically independent (from services that disseminate pornographic content). The services must in under no circumstance have access to the data used to verify the age of the user.
- carry-out the verification in two separate steps, i.e. identification and authentication (of the person identified), and for each usage session.

An age verification system using 'double anonymity', i.e. based on the intervention of an independent third party, should not allow the services to recognise a user who has already used the system on the basis of the data generated by the age verification process. The use of age verification systems using 'double anonymity' should not allow these services to know or infer the source or method for obtaining the proof of age involved in the process of verifying a user's age.

For app-based systems (e.g. digital identity wallet app), the app certifies and generates the proof of age for the user, who can then provide the evidence to the visited website or platform. In other cases, the proof is issued by a specialised entity (or an entity that has identified the user in another context, but is in any case certified), and communicated to the user, who then presents it to the platform. The platform must then analyse the proof, and provide or deny access.

The authority clarifies that its approach is technology neutral and that platforms remain free to choose the system, provided that the systems comply with a set of principles.

3.4 Germany

According to Germany's Interstate Treaty on the Protection of Minors[27], **pornographic content, certain listed content and content that is obviously harmful to minors** can only be distributed on the internet if the provider ensures that only **adults** have access to it by means of "closed user groups"[28].

Age verification systems are used as one way to control closed user groups. The rules apply to «telemedia providers» i.e. all electronic information and communications services, except telecoms services and to VSPs. Streaming/VOD providers are covered as well as operating systems and search engines.

The technical requirements for these systems are higher than the requirements for technical means that prevent access to content that is only likely to impair the development of minors. Accordingly, age verification to be used for closed user groups must involve two inter-related steps:

- identification: proof of age must be carried out via personal identification (face-to-face contact)

[27] https://www.die-medienanstalten.de/service/rechtsgrundlagen/jugendmedienschutz-staatsvertrag/
[28] Article 4(2) of the Treaty.

- authentication: only identified and age-verified persons are granted access during the individual usage process.

To give certainty, the Commission for the Protection of Minors in the Media (KJM) can check and approve whether the "concepts" for the technical protection of minors meet the legal requirements. The KJM published criteria for the evaluation of these concepts.[29] It has approved 50 complete solutions and 48 partial systems (called modules)[30]. The other key features of the German system is that this evaluation process is done at the request of service providers and the main responsibility for implementing the verification process lies with the content provider, which ultimately needs to make sure that pornographic content (and other content harmful to minors) is accessed only by adults.

[29] https://www.kjm-online.de/themen/technischer-jugendmedienschutz/entwicklungsbeeintraechtigung/. The KJM includes age evaluation for one-time use and for repeated use.
[30] https://www.kjm-online.de/themen/technischer-jugendmedienschutz/unzulaessige-inhalte/

4. Internal Market Issues

In the context of the regulatory transparency procedures set up under Directive 2015/1535,[31] Member States have notified to the European Commission their draft legislative initiatives on the protection of minors, including on age verification. Beyond the countries covered in this report, other countries, including Hungary and Spain have also notified draft laws covering these areas.

The European Commission has been issuing either detailed opinions or non-binding comments[32] to most of the notifying Member States, on the grounds that the draft national rules:

- are incompatible with the country of origin principle of the Electronic Commerce Directive[33] because they seek to impose obligations on 'information society services' offering their services in France, in addition to those imposed by the Member State where they are established; and/or
- undermine the full harmonisation approach of Article 28 DSA (a regulation does not normally require national implementation legislation; and/or
- overlap with the Commission's monitoring and enforcement powers of the very large online platforms.

France received a detailed opinion from the Commission following the notification of its draft rules leading up to the adoption of the SREN Law.[34] France argued in its response that the age verification measures of the SREN law were proposed in the context of the transposition of Article 28b AVMSD, and that the rules apply to VSPs and to services over which the service providers have editorial control (hence services that are not in the scope of the DSA). The Commission in its reaction noted that the envisaged rules are not limited to VSPs but also cover other types of online platforms that are covered by the DSA. However, both the European Commission and the French authorities seem to agree that the French rules can be adopted so long as France revises its framework when sufficiently precise rules exist at the EU level for effective age verification. Also, it must be noted that the French rules on age verification and the removal of pornography apply to service providers based in France and outside the European Union. They also apply to providers established in another EU member state if the conditions to derogate from the country of origin principle are met. In this case, the measures apply three months after the publication of a joint ordinance by the ministers for culture and for digital technologies designating the service providers involved. Arcom can propose the designation to the ministers. France will probably notify another draft application decree of the SREN Law which foresees

[31] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification) (Text with EEA relevance) OJ L 241, 17.9.2015, p. 1–15
[32] Detailed opinions have the effect of extending the standstill period (during which the Member State needs to refrain from adopting the final rules) by one additional month. During this period, the Member State needs to explain the follow up action it intends to take in response to the detailed
[33] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') OJ L 178, 17.7.2000, p. 1–16

[34] https://technical-regulation-information-system.ec.europa.eu/en/notification/24221/message/105804/EN

that VLOPs established in Cyprus (Pornbub, Stripchat) and the Czech Republic (XNXX, XVideo) will need to comply with Arcom's technical rules on age verification.

France did not receive a formal opinion following the notification of the law on the digital majority but the press reports that former EU Commissioner Thierry Breton sent a letter to the French minister for Europe and Foreign Affairs in which criticisms were voiced against the draft law.[35]

The Commission had no comments following the notification of the draft Online Safety Code, which online concerned VSPs established in Ireland.[36]

Germany received a detailed opinion[37] on 1 July 2024 in which the Commission expressed serious concerns as to whether the draft Interstate Treaty on the Protection of Minors and Broadcasting is in line with the country of origin principle of the Electronic Commerce Directive or with the DSA.

Regarding the incompatibility with Article 3 of the Electronic Commerce Directive, the Commission notes that the provisions of the notified draft apply to information society services offering services in Germany and irrespective of their state of establishment and that despite the fact that the German authorities have stated their intention to enforce the notified draft on providers established outside of Germany on the basis of individual measures adopted by competent authorities, this is not reflected in the version notified by Germany.

Regarding the DSA, the Commission recalls that the Regulation establishes fully harmonised rules for a for a safe, predictable and reliable online environment. In particular, the Commission recalls that the protection of minors, a particularly vulnerable category of recipients of online intermediary services, is an essential aspect of the DSA. The Commission also recalls that, being a Regulation, the DSA does not allow for additional national requirements unless otherwise expressly provided. The Commission also notes that "the notified draft entrusts the supervision and enforcement of the notified draft, including the provisions falling within the fully harmonised field of the DSA, to the German media authorities (at various levels). This supervision and enforcement system under the notified draft would also apply with regard to service providers outside the jurisdiction of Germany and very large online platforms or very large online search engines in as much as they are covered by the scope of the notified draft. The Commission calls on the German authorities to ensure that the final law is aligned with the supervision and enforcement architecture of the DSA".

In short, the margin of manoeuvre of Member States wanting to impose age assurance obligation on platforms appears quite limited. The only option for Member States seems to be to impose such obligations on VSPs established in their member state. All other scenarios appear to be either in breach of the full harmonised approach of the DSA and - if the rules target information society service providers established in other Member States - of the Electronic Commerce Directive. The Commission also notes enforcement issues (see also the companion Issue Paper 'Charting the Path for Protection of Minors under the DSA').

[35] https://www.linforme.com/tech-telecom/article/majorite-numerique-influenceurs-la-lettre-incendiaire-de-thierry-breton-au-gouvernement_1056.html
[36] https://www.cnam.ie/statement-on-the-online-safety-code/
[37] https://technical-regulation-information-system.ec.europa.eu/de/notification/25746/message/108751/EN

5. Age Assurance in the UK and in Australia

5.1 UK

In the UK, following the adoption of the Online Safety Act[38], the regulator for the communications sector, Ofcom, is developing Children's Safety Codes with recommended measures that providers of services likely to be accessed by children need to take to comply with the Act.[39] Generally, Ofcom expects much greater age assurance, so that services know which of their users are children. All services which do not ban harmful content and those at higher risk of it being shared should implement "highly effective age assurance"(HEAA). Ofcom proposes that user to user (U2U) services use HEAA to restrict access to the whole service or from encountering certain types of identified content.

HEAA should be used to control access to an **entire service** if the service in question is deployed by a:

- U2U service whose principal purpose is the hosting or the dissemination of one or more kinds of PPC (Primary Priority Content: **pornographic content, suicide and self-harm content and eating disorder content**);
- U2U services whose principal purpose is the hosting or the dissemination of one or more kinds of PC (Priority Content: **abuse and hate content, bullying content, violent content, harmful substances content; dangerous stunts and challenges content**) AND who are high/medium risk for one or more of those kinds of PC.

HEAA should be used to prevent children from encountering **PPC identified** on a service:

- if the U2U service is not hosting or disseminating one or more kinds of PPC and which do not prohibit one or more kinds of PPC
- if the U2U service whose principal purpose is not the hosting or the dissemination of one or more kinds of PC; AND which do not prohibit one or more kinds of PC; AND are high/medium risk for one or more kinds of PC that they do not prohibit.

Interestingly, Ofcom considers that it is important to set consistent expectations for how service providers that allow pornographic content on their service implement HEAA to prevent children from encountering pornographic content, regardless of the type of service (U2U services or publishers of content).

All U2U services and search services need to carry out a **children's access assessment** to assess if the service (or part of it) is likely to be accessed by children. If the service is likely to be accessed by

[38] https://www.legislation.gov.uk/ukpga/2023/50/enacted
[39] https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/284469-consultation-protecting-children-from-harms-online/associated-documents/vol5-what-should-services-do-to-mitigate-risks.pdf?v=336054#page=34?v=336054#page=34

children, it will need to conduct a child risk assessment within a time that is also specified by Ofcom (3 months).

Ofcom does not recommend the use of specific age assurance methods but recommends that services take steps to fulfil criteria of technical accuracy[40], robustness[41], reliability[42] and fairness[43] (to ensure that their age assurance process is highly effective). Also, when implementing age assurance, the service providers need to make sure that age assurance is easy to use, including by children of different ages and with different needs. It is also desirable to ensure interoperability between different kinds of age assurance.

Ofcom has put forward a non-exhaustive list of kinds of age assurance that it considers possibly as highly effective[44], while also listing age assurance methods that are not highly effective[45]. Age assurance methods are developing rapidly and list of highly effective age assurance methods will expand over time. Like in other jurisdictions, Ofcom notes that age assurance methods involve the processing of personal data and hence, they should respect the requirements of the UK's data protection regime.

Ofcom has been assessing the age assurance measures on adult VSPs under the VSP regime that derived from the implementation of Article 28b AVMSD. This regime will be repealed once Ofcom's final codes on the protection of minors are adopted in April 2025.

On 16 January 2025, Ofcom published guidance for the industry on effective age checks to prevent children from encountering online porn and to protect them from other harmful content. Porn services have until July 2025 (at the latest) to introduce them and Ofcom will monitor compliance through an **enforcement programme**.[46]

Interestingly also, the guidance specifies that services that publish their own pornographic content should put in place HEAA immediately, including certain Generative AI tools.

5.2 Australia

Australia enacted on 10 December 2024 the Online Safety Amendment (Social Media Minimum Age) Act 2024[47] which foresees that service providers must take reasonably steps to prevent children under 16 from being present on certain social media or from opening new accounts. Technically, the act modifies the Online Safety Act 2021, which established the eSafety Commissioner, while also setting

[40] This refers to the degree to which an age assurance method can correctly determine the age of a user under test lab conditions.
[41] This refers to the degree to which an age assurance method can correctly determine the age of a user in unexpected or real-world conditions.
[42] This refers to the degree to which the age output from an age assurance method is reproducible and derived from trustworthy evidence.
[43] This refers to the extent to which an age assurance method avoids or minimises bias and discriminatory outcomes.
[44] Open banking, photo-ID matching, facial age estimation, mobile network operator age checks, credit card checks, reusable digital ID services.
[45] Self-declaration of age, age verification through online payment methods which do not require a user to be over 18; and general contractual restrictions.
[46] https://www.ofcom.org.uk/online-safety/protecting-children/age-checks-to-protect-children-online/. The enforcement programme is available here : https://www.ofcom.org.uk/online-safety/protecting-children/enforcement-programme-to-protect-children-from-encountering-pornographic-content-through-the-use-of-age-assurance/
[47] https://www.legislation.gov.au/C2024A00127/asmade/text

up measures to combat cyberbullying towards children, cyber-abuse towards adults and the non-consensual sharing of intimate images.

The Online Safety Amendment (Social Media Minimum Age) Act 2024 will take affect within one year, on a date to be specified by the minister, with important details to be specified by the minister in charge and the eSafety Commissioner. Service providers that fail to comply with the age restrictions will face civil penalties. The minister in charge needs to specify (through legislative rules):

- The services in scope (the eSafety Commissioner will provide advice); and
- The type of information that cannot be collected (the eSafety Commissioner and the Information Commissioner will provide advice).

The eSafety Commissioner will formulate guidelines on age verification systems, following a consultation.

Australia's Online Safety Act requires that industry associations regulate certain types of online material through the development of codes of practices that need to be registered with the eSafety Commissioner, to become binding on all industry participants. If a code fails to meet the requirements of the law, the regulator can develop its own legally binding rules.

Phase 1 codes have been finalised[48] and are aimed at helping online service providers comply with class 1A and 1B material (i.e. the most seriously harmful online content, such as child sexual exploitation material and pro-terror material), while the **Phase 2 Code**, focussing on class 1C and class 2 material such as online pornography that is inappropriate for children, is in the course of development.

Australia's Phase 1 Code includes a special requirement for app distributors which is to 'make age and/or content ratings information about third-party apps available on the app distribution service to Australian end-users at the time those third-party apps are released on the app distribution service'.[49]

The eSafety Commissioner issued a position paper on the development of phase 2 industry codes in July 2024[50]) The regulator proposes that age rating systems are enforced on app distribution platforms, which could mean that they should take steps to confirm end-user's ages.

It is also noteworthy that in Australia, for theses codes, a wide range of services are targeted, such as equipment services, search, and instant messaging services.

It must be noted that in Australia, content is **classified** according to the National Classification Scheme.[51] For instance class 2 material includes X18+ or R18+ content that may be harmful to children.

[48] https://www.esafety.gov.au/sites/default/files/2024-12/Phase-1-Codes-1A-and-1B-Regulatory-Guidance-Updated-Dec2024_2.pdf?v=1735996489216

[49] Measure 3 of the Phase 1 App Distribution Platform Distribution Code, https://www.esafety.gov.au/industry/codes/register-online-industry-codes-standards

[50] https://www.esafety.gov.au/sites/default/files/2024-07/Development-of-Phase-2-Industry-Codes-under-the-Online-Safety-Act-eSafety-position-paper_0.pdf?v=1735996489216

[51] https://www.classification.gov.au/about-us/legislation

This includes online pornography, high-impact depictions of violence or drug use, and from September 2024, computer games with simulated gambling, such as social casino games.

The eSafety Commission has already conducted some research in the context of the development of the Phase 1 and 2 Codes, including on age verification. It published an Age Verification Roadmap which examined approaches to address the risks and harms associated with children accessing online pornography. [52] Importantly, as any initiative on the matter in the EU, the Australian regulator sought to take "a human rights based approach, considering the rights, best interests and evolving capacities of children, as well as the rights of parents, carers, and other adults, including sex workers and performers and producers of online pornography… which aligns with the United Nations Committee on the Rights of the Child, supporting the child's best interests while also respecting the rights of adults to consume and produce pornography in a safe and lawful manner".

The regulator recommended that the government should undertake work on trial age assurance technologies before mandating their use. The aim of the trial is to support industry about how industry is expected to confirm the age of users.[53]

This overview of these national developments shows that although the models examined have similar goals (except Australia, which is moving towards an outright ban of the use of social media for children under the age of 16), age assurance is addressed in different ways. There would be merit in having a more structured regulatory alignment across regions of the world, given the global reach of some of the players. For this, the EU should develop its own model and attempt to put an end to national fragmentation.

[52] https://www.esafety.gov.au/about-us/consultation-cooperation/age-verification#roadmap-and-background-report
[53] The eSafety Commission published an issue paper on age assurance in July 2024, which is available at https://www.esafety.gov.au/industry/tech-trends-and-challenges#age-assurance

Summary Table of National Systems

	Type of content	Services in scope	Type of age assurance	Role of regulator	Other features
Australia	Certain social media	Certain social media	To be determined	▪ To formulate guidelines ▪ To determine the services in scope	
	-Seriously harmful online content - class 1C and class 2 material such as online pornography that is inappropriate for children	Also app distributors Search Equipment services Messaging services etc.	Regulator proposed that government should conduct a trial of age assurance	▪ Register industry codes of conduct	
France	Pornographic content	All websites that make content available	▪ Double anonymity Prevent circumvention ▪ Avoid discrimination ▪ Respect personal data ▪ Ensure verification each time the service is accessed	▪ Sets technical requirements for age verification ▪ Can request service providers to carry out audits ▪ Enforcement and blocking orders	Sanctions (up to 3% of worldwide annual turnover) Blocking orders can be ordered by regulator
Germany	Pornographic content and certain listed content that is obviously harmful to minors	All services except telcos	▪ The overall aim of the systems are set by law (closed user groups)	▪ Regulator can check and approve systems	Although the regulator may check that the system complies with the law, the responsibility for deploying the system lies with the service provider

Ireland	In particular, pornography and extreme gratuitous violence.	VSPs that do not preclude the upload of adult only video content	Not specified beyond that it needs to be an effective method of age assurance	Guidance	Complaints systems on VSPs need to deal with possible issues in relation to age assurance
Italy	Pornographic images and videos	Website operators, including and VSPs	Needs to be certified and technically independent from service provider Double anonymity	Sets procedural and technical measures	Operators that disseminate content must tell regulator who is in charge of age verification
UK	Pornographic content, suicide and self-harm and eating disorder content + abuse and hate content, bullying content, violent content, harmful substances content; dangerous stunts and challenges content	User to user services Publishers of pornography	Highly effective age assurance	▪ Regulator publishes non-exhaustive list of types of systems ▪ Detailed enforcement programme	Detailed enforcement programme

6. Critical Appraisal of the EU framework

This report shows that there is a significant amount of national fragmentation in the EU on age assurance. This could undermine the protection of minors since, depending on where the digital service provider is established, the level of protection will be different. This is situation is not optimal either for pan-European service providers as they will incur significant compliance costs depending on the market.

Multiple factors explain this situation, some of which are linked to the EU-level rules themselves. This section reviews some of the issues and puts forward recommendations on possible solutions.

More clarity at the EU level on the type of services/content that should not be accessed by minors

A major difficulty with the EU level rules is that there is no EU-wide standard on the type of services or content that should not be accessed by minors. To date, there is no EU-wide definition of what constitutes harmful content leaving this to be determined at national level. Although it is extremely complex to define age-appropriate content across the Member States, which have culturally diverse communities, it may be possible to agree at the EU level that certain types of services or content are certainly harmful to children.

This approach is not entirely new at the EU level since in relation to TV, on-demand services and VSP, the AVMSD specifies that the most harmful content, such as gratuitous violence and pornography should be subject to the strictest measures.

The DSA refers to harmful content in a few instances but does not explain what harmful content covers, nor does it refer to particular types of harmful content for minors.

We see that at national level restricting access to pornography is a common concern, and that this takes place at the service level (e.g. Germany, France and Italy). Some of the legislations are also aimed at restricting access to other types of very harmful content.

The deployment of robust age assurance systems to prevent minors from accessing such content comes at a cost and there are trade-offs (such as additional personal data may need to be processed, the economic burdens of putting the systems in place, which could be difficult for new entrants or smaller companies, the fact that minors may be deprived from accessing etc).

These are not easy questions, but we see that on balance, something needs to be done, because the risk to minors seems high and because the risk of internal market fragmentation is also high.

We recommend that the guidelines seek to single out pornography (and possibly other types of very high-risk content such as gratuitous violence, suicide and self-harm). In relation to this content, the EU could recommend that effective age assurance technology **needs** to be used, provided the system complies with a set of principles such as the respect privacy and personal data in particular.

The guidelines should also seek to single out a **common age** to access such content. The age could be the age of majority (i.e. 18 in most Member States) or a younger age such as the age of consent (the age varies but according to Wikipedia, the oldest age in the EU is 17).

If the Member States continue to apply their own national systems or if the platforms do not comply, the EU may need to adopt a **targeted legislation** to specify these elements.

In relation to other (less serious forms of) harmful content, age verification is probably not desirable because of the high trade-offs would probably not outweigh the benefits of protecting minors from harm, also giving their fundamental right to access the online information. Other less intrusive forms of age assurance such as age estimation coupled with age-appropriate design would probably be sufficient.

The **content classification/age ratings** attached to different types of content are useful tools to help users to navigate through different types of content that could be harmful to minors, depending on their age groups. However, they are not easy to put in place in an environment where there is a lot of user generated content bearing in mind that the DSA includes a no general monitoring obligation.[54] In some industries (audiovisual and gaming in particular) there are effective voluntary age rating systems[55] but this is not easy to replicate on platforms where the service provider does not have editorial control. In any event, the guidance could also seek to shed some light on these questions.

The articulation between the rules of the AVMSD and the DSA is not optimal and should be reassessed

VSPs are potentially covered by both sets of rules. A VSP is defined in Article 1 AVMSD as a service that has as its principal purpose (or as a dissociable section) or an essential functionality the provision of "programmes, user-generated videos, or both, to the general public, for which the video-sharing platform provider does not have editorial responsibility"… and "the organisation of which is determined by the video-sharing platform provider, including by automatic means or algorithms in particular by displaying, tagging and sequencing". This definition overlaps with that of an online platform under the Article 3 DSA.[56]This means that VSPs would potentially need to respect both sets of rules.

Although there may not be a direct incompatibility between the rules, since the AVMSD is a minimum harmonisation directive, the Member States are allowed to impose on VSPs established in their member states more detailed or stricter measures. This could therefore create a situation where age assurance could be mandated by a Member State for VSPs, whereas for other types of platforms, this would not be the case. This is in the spirit of the AVMSD, and the DSA itself recognises in recital 10 that the regulation should be "without prejudice" to other acts of Union law regulating the provision of information society services in general, regulating other aspects of the provision of intermediary services in the internal market or specifying and complementing the harmonised rules set out in this Regulation, such as the AVMSD (including its rules regarding VSPs). The DSA on the other hand, is aimed at fully harmonising the areas it covers, leaving no space for the Member States to introduce added rules.

[54] Article 8 DSA
[55] PEGI for the gaming industry and Kijkijzer for audiovisual content.
[56] 'online platform' means a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public, unless that activity is a minor and purely ancillary feature of another service or a minor functionality of the principal service and, for objective and technical reasons, cannot be used without that other service, and the integration of the feature or functionality into the other service is not a means to circumvent the applicability of this Regulation.

Although the texts themselves recognise the coexistence of the rules, **in practice, the situation is not optimal:**

- **First**, it is legitimate to question the logic behind having a different legal treatment for VSPs compared to other types of online platforms. The scope of the AVMSD was broadened in 2018 to introduce rules to protect viewers and minors when they view audiovisual content on platforms, the logic being that audiences should be protected in a similar way than when the watch television and audiovisual media services on demand. Now that similar rules are introduced in the DSA for all types of online platforms, the rules of the AMVSD and how they have been transposed and put into application at the national needed to be assessed, to examine if they are still needed.
- **Second**, the **oversight of the rules will be different and may lead to complex situations**. In the case of the oversight and enforcement of the rules derived from the AVMSD, it is up to the regulatory authority of the country of establishment to assess whether measures chosen by VSPs are effective on a case-by-case basis. In practice the media regulator exercises this power and in case of breach of the rules, those derived from the transposition of the AVMSD will apply. In the case of enforcement of the rules derived from the DSA, the competent authorities designated under the DSA and the Digital Service Coordinator (DSC) are competent at the national level. For VLOPs and VLOSEs, the European Commission is the sole enforcer of Articles 34 and 35 on risk assessments and risk mitigation measures, whereas for the enforcement of the other rules, the competent authorities and the DSCs of the country of establishment are still potentially the enforcers (except if the Commission decides to take the lead).

This re-assessment should take place in the context of the upcoming review of the AVMSD which needs to take place by 19 December 2026 at the latest[57]. The DSA foresees that by 17 November 2025, the Commission must report on the way the regulation interacts with other legal acts.[58]

However, nothing precludes the European Commission from addressing these overlaps in the meantime.

Different rules for different types of intermediaries, content types and targeted users?

The tailored due diligence obligations introduced by the DSA are laudable and is a great step forward. Different obligations are introduced according to the type of intermediary, with more stringent obligations to be complied with by respectively, mere conduit, caching, hosting, online platforms, and very large online platforms and search engines.

However, within these categories, the obligations do not differ, according to the type of content they convey, nor according to their expected category of users. Porn platforms are subject to the same obligations as any other type of online platform, even if the risk assessments and risk mitigation measures would need to be tailored to the specific risk incurred by minors. Likewise, article 28 DSA

[57] Article 33 AVMSD.
[58] Article 91 DSA.

contains a proportionality criterion, but other than that that the DSA does not treat such platforms - in a different manner.

Also, we note that under the DSA, only the VLOPS and VLOSES need to carry out **risk assessments**. However, this could be a useful tool for other platforms as well - especially **child specific risk assessments**. The European Commission could recommend in its upcoming guidelines that services that are available to users under the age of 18 could conduct risk assessment to examine whether (and if so, which) age assurance systems could be put in place.

Some online platforms argue that **app stores** (such as Apple App store and Google Play, which allow users to download applications on their devices) should be subject to added age assurance obligations. App stores assign age content ratings and require users to log in with their accounts. This means that they could in principle verify the age of users, which would have significant advantages as they often serve as gatekeepers for app downloads. Australia's Phase 1 Code includes a special requirement for app distributors which is to make age 'make age and/or content ratings information about third-party apps available on the app distribution service to Australian end-users at the time those third-party apps are released on the app distribution service'.[59] For Phase 2 Codes (regulating access to porn platforms for instance) the regulator proposes that age rating systems are enforced on app distribution platforms, which could mean that they should take steps to confirm end-user's ages.

This line of thought does not alleviate the need for the online platforms that are not app stores from ensuring a high level of privacy, security and safety of minors on their own services but since this added responsibility is also under consideration in Australia and the proposed CSAM regulation, the option of imposing added responsibilities on app stores merits more analysis.

Some services are out of scope of the EU legislative framework

As discussed in Section 2 some potentially high-risk services are not covered by the DSA (or by the AVMDS) such as online shops selling age restricted substances, adult content websites (with editorial responsibility), gambling websites and search engines (that are not very large or that only generate natural/generic links) . For these services, age verification obligations (if any) will only derive from national legislation, which will once more undermine the functioning of the internal market and hinder the deployment of pan-European services. Where it is proven that these gaps present risks for child protection, they should be filled to avoid an uneven level of protection of children.

What level of state intervention in age assurance systems?

The report shows various levels of regulatory intervention on the type of age assurance system to be used, even if no country imposes a given technology.

First, there are countries where the system is entirely left to the service providers, with a list of requirements to be fulfilled (Ireland) and/or a list of acceptable or non-acceptable systems (UK).

Second, there are countries where the level of intervention of the regulator is higher. France, Germany and Italy have a stronger oversight model as they are putting in place systems where the regulator

[59] Measure 3 of the Phase 1 App Distribution Platform Distribution Code, https://www.esafety.gov.au/industry/codes/register-online-industry-codes-standards

needs to specify technical parameters, or where there is a need to conduct independent audits, or where there is the possibility to ask for clearance that the systems are in line with the legal requirements.

The EU should decide which of these models it would like to embrace.

EU policy decisions should be taken on the role to be given to the European Commission and to national competent authorities (if any). The sanctions in case of non-compliance (France provides that ISPs can be asked to block access to non-compliant services) could also be considered.

At the very minimum the European Commission could adopt a list of best practices for age assurance/verification tools. If it decides to oblige certain platforms to deploy age verification by adopting EU binding legislation, this legislation would probably also need to specify the role of the European Commission in setting the technical parameters, possibly by fostering EU standards[60].

A clear mention could in any event be made in the guidelines on consequences of using the European Commission's technical system developed under the universal age verification solution which is currently under development.

The rights of the child and other guiding principles

The rights of the child as envisaged in the EU Charter on Fundamental Rights (especially Article 24), the European Declaration on Digital Rights (in particular points 20-22), and the UN Convention on the Rights of the Child should remain the guiding principles when considering how to protect children from accessing services or content online.

A number of other core principles[61] on which age assurance solutions could be based could also be clearly articulated in the Commission's guidelines on Article 28 DSA and in any forthcoming legislation. The Commission could also specify if age verification solutions will also need to comply with the requirements of the EU Accessibility Act[62] and with the Cyber Resilience Act[63] once these enter in application.

[60] Such as the IEEE standard for Online Age Verification, https://standards.ieee.org/ieee/2089.1/10700/
[61] In particular, privacy preserving; proportionate to the risks and purpose, easy to use, secure; accessible; inclusive and interoperability.
[62] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L0882
[63] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202402847

7. Conclusion

This report highlights that the EU rules on age assurance are embryonic, whereas they are an important part of the ecosystem to ensure the protection minors of minors online. The Member States are therefore filling the gaps, which is creating internal market fragmentation, implementation difficulties for platforms that need to comply with the DSA and for competent authorities that need to enforce the rules.

The Commission's guidelines on Article 28 DSA are certainly needed but it is unclear, given their non-binding nature, if they will put an end to the appetite for national rules.

There are also some shortcomings in the EU legislation, since some services are not covered by the DSA (nor are they covered by the AVMSD). The articulation between the DSA and the AVMSD is not clear, which is could also lead to application difficulties. These difficulties will probably need to be resolved by legislation.

Turning to age assurance per se, and when looking at developments in other Member States (and regions of the world), we see that one of the most pressing issues is to decide if age verification should be mandated to prevent minors from accessing adult content services and possibly other high-risk content.

The EU should also clarify the level of state intervention for age assurance technology: none, mere guidance or a stronger oversight potentially with requirements to be specified, accreditation or auditing of technology. It also needs to decide on what are the respective roles of the European Commission and the national competent authorities.

Finally, the rights of the child and other guiding principles should be clearly articulated in the EU's normative system when adopting or recommending rules on age assurance.

This clarity would not only contribute to the protection of minors online but it would also allow pan-European services to be offered with more certainty across the EU. Ultimately, this would also enable the EU to develop its own 'regional approach' which could then be used to find some form of global alignment across different regions of the world.

Further Reading

European Commission: Directorate-General for Communications Networks, Content and Technology, New Better Internet for Kids Strategy (BIK+) – Compendium of EU formal texts concerning children in the digital world – 2024 edition, Publications Office of the European Union, 2024, **https://data.europa.eu/doi/10.2759/90437**

The protection of minors on VSPs: age verification and parental control, European Audiovisual Observatory, Strasbourg, 2023

Livingstone, S., Nair, A., Stoilova, M., van der Hof, S., & Caglar, C. (2024). Children's Rights and Online Age Assurance Systems: The Way Forward. The International Journal of Children's Rights, 32(3), 721-747. https://doi.org/10.1163/15718182-32030001

Research report : Mapping age assurance typologies and requirements, February 2024; Written by: Mohammed Raiz Shaffique LLM and Professor Simone van der Hof Center for Law and Digital Technologies (eLaw) Leiden University, Leiden, The Netherlands Part of the Better Internet for Kids (BIK) project coordinated by European Schoolnet (EUN) and commissioned by the European Commission.

Issue Paper

Protection of Minors: Age-Appropriate Design

Miriam Buiten
Christoph Busch

March 2025

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.[64] 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.[65]

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

[64] 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.
[65] 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.

to platforms, to ensure children's safety and positive experiences once using online services.[66] 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 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.

[66] 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.

- 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.[67]

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.[68]

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

[67] 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.
[68] See further below on Goals.

parental consent where necessary. Equally important is **content recommendation**[69] **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.

[69] 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.[70] This means there is no single, fixed definition of what best serves children's interests online; instead, it requires careful, context-sensitive consideration.[71] 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.[72] A child-centred approach avoids seeing children only as vulnerable victims or prioritising their protection from risk at the expense of their online opportunities.[73] 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.[74] 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.[75]

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

[70] 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.
[71] General comment No. 20 on the implementation of the rights of the child during adolescence, UN Committee on the Rights of the Child (2016).
[72] 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
[73] 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/
[74] 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.
[75] 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

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.[76] 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.[77] 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.[78] 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.[79]

- 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.[80]
- **Encouraging responsibility among platforms:** Establishing expectations that platforms proactively consider the needs of children in their design and operational choices.

[76] 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.

[77] 5Rights Foundation (2019). Towards an internet safety strategy. 5Rights. https://5rightsfoundation.com/uploads/final-5rightsfoundation-towards-an-internet-safety-strategyjanuary-2019.pdf

[78] 5Rights Foundation (2019). Towards an internet safety strategy. 5Rights. https://5rightsfoundation.com/uploads/final-5rightsfoundation-towards-an-internet-safety-strategyjanuary-2019.pdf

[79] 5Rights Foundation (2019). Towards an internet safety strategy. 5Rights. https://5rightsfoundation.com/uploads/final-5rightsfoundation-towards-an-internet-safety-strategyjanuary-2019.pdf

[80] 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.[81]

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

[81] 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.

- 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.[82] Initial steps toward developing such a framework are outlined further below.

[82] 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:[83]

- **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.[84] 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,"[85] 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.

[83] 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.
[84] [84] 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.
[85] 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.[86] 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.[87]

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.[88] Psychological and developmental harm may result from violent content,[89] bullying, or the influence of recommender systems,[90] where they amplify problematic material by repeatedly pushing similar content personalised for children.[91] Additionally, exposure to inappropriate content, such as adult material, and the promotion of addictive behaviours further threaten children's healthy development and well-being.[92]

---

[86] 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.

[87] 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.

[88] 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.

[89] 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

[90] 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.

[91] 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/.

[92] 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. (2022). Young users' social media addiction: causes, consequences and preventions. Information Technology & People, 35(7), 2314-2343.

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.[93] **Transparency**: Clearly communicate terms and conditions in a way that children and their guardians can understand,[94] as well as transparent information on risk and actual harm that has occurred on the service.[95]
- **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.[96]
- **Safe Defaults**: Ensure safety is embedded by default in design choices:[97]

[93] 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
[94] 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/.
[95] OECD, 13-14.
[96] 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.
[97] 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.

- **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.[98]
- **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.[99]

- **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. [100]

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.

---

[98] 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?.
[99] 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.
[100] 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.

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		
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.	**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.	**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.

Default Settings		
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.	**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.	**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.

Recommender Systems		
Best Practice: A video platform for children curates diverse, age-appropriate content and provides tools for parents and children to adjust content preferences. It also excludes advertising or sensitive topics like gambling or violence.	**Grey Practice:** A gaming site shows non-targeted advertisements to users, including older children. While the ads aren't inappropriate, they lack tailoring to children's age groups, potentially exposing younger users to irrelevant or slightly confusing content.	**High-Risk Practice:** A music-streaming app recommends inappropriate content, such as explicit lyrics or videos with violent themes, based on user activity without sufficient safeguards for younger users.

Interface Design		
Best Practice:	**Grey Practice:**	**High-Risk 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.	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.	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.

Data Privacy & Security		
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.	**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.	**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.

Parental Controls & Child Autonomy		
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.	**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.	**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.

Behavioural Nudges		
Best Practice: A mindfulness app for children provides regular break reminders and gamifies educational activities to encourage balanced usage and meaningful engagement.	**Grey Practice:** A gaming app uses suggestive nudges, such as "Keep playing to unlock rewards," which increase engagement but do not cross into manipulation.	**High-Risk Practice:** 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.

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.

cerre Centre on Regulation in Europe

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