



**DSA IMPLEMENTATION  
FORUM 2024: CHARTING THE  
PATH FOR THE PROTECTION  
OF MINORS UNDER THE DSA**

---

*March 2025*

---

Miriam Buiten  
Michèle Ledger



cerre

Issue Paper

# **DSA Implementation Forum 2024: Charting the Path for the Protection of Minors under the DSA**

Miriam Buiten  
Michèle Ledger

March 2025



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

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

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

info@cerre.eu – www.cerre.eu



# Table of Contents

<b><u>ABOUT CERRE.....</u></b>	<b><u>3</u></b>
<b><u>ABOUT THE AUTHORS .....</u></b>	<b><u>4</u></b>
<b><u>1. CHARTING THE PATH FOR PROTECTING MINORS UNDER THE DSA.....</u></b>	<b><u>5</u></b>
1.1 DSA OBLIGATIONS.....	6
<b><u>2. COMMON THEMES.....</u></b>	<b><u>7</u></b>
2.1 INTERACTION BETWEEN AGE ASSURANCE AND AGE-APPROPRIATE DESIGN .....	7
2.2 OVERALL COHERENCE OF THE REGULATORY FRAMEWORK .....	9
2.3 INTERNAL MARKET FRAGMENTATION.....	9
2.4 ECOSYSTEM OF OVERSIGHT BODIES .....	9
<b><u>3. OUTLOOK .....</u></b>	<b><u>11</u></b>





## About CERRE

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

CERRE's added value is based on:

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

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



## About the Authors



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



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.



# 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 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?<sup>1</sup>

**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

---

<sup>1</sup> DSA Art. 8



tension: platforms are required to apply age-appropriate measures, yet there is little concrete 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.<sup>2</sup>

These approaches reflects 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.

---

<sup>2</sup> Art. 4.1 of the Dutch Media Law



## 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 Media Services Directive (AVMSD)<sup>3</sup> 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

---

<sup>3</sup> 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





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**.<sup>4</sup> This will require careful coordination to address the evolving challenges.

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.

---

<sup>4</sup> G. Monti and A. de Streel, *Improving institutional design to better supervise digital platforms*, CERRE Report, January 2022.



### 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.



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

