

The DSA Guidelines for the protection of minors online

**Policy Briefing
for members**



Eurochild
Putting children at
the heart of Europe

November 2025

The DSA Guidelines for the protection of minors online

Introduction

This policy brief outlines the key provisions of the Digital Services Act Guidelines for the Protection of Minors and their implications for child rights organisations and national legislators. The aim of this document is to support Eurochild members' advocacy in the national implementation of the Digital Services Act requirements for online child safety.

Background

The Digital Services Act (DSA) is the legislative cornerstone of EU action to ensure safer online environments for children. It includes obligations for big online platforms to assess and mitigate the risks they pose to children (Art 34 and 35), and for all online platforms to ensure a “high level of privacy, safety and security for minors” (Art 28). It also bans targeted advertisement to minors.

In order to clarify how online platforms should comply with providing a high level of safety, privacy and security according to article 28, The European Commission adopted guidelines on 14 July 2025. These Guidelines aim to support online platforms and regulators interpret and implement Article 28 obligations, providing a common reference across EU Member States. They provide a practical benchmark for national Coordinating Authorities to evaluate compliance of these platforms with regards to the DSA. Therefore, it is not a new set of rules, but rather specific recommendations that clarify the obligations that platforms are already subject to under the DSA.

In simpler terms, while the Guidelines don't have the force of law, they indicate what is considered good practice both for online platforms to comply with and for regulators to enforce the DSA. They are therefore a powerful tool for child rights organisations to hold platforms and regulators to account.

Key provisions

The Guidelines apply to all online platforms accessible to minors either by terms and conditions, because the provider is aware of children using the service or because it does not effectively prevent minors from accessing the service – i.e., services targeting adults who do not implement effective age assurance.

The Guidelines provisions provide a list of recommendations, but they are non-binding, not exhaustive and do not pre-empt online platforms from implementing other measures that

may be considered to deliver safety and privacy for minors. They serve as a reference for online platforms, regulators and courts: compliance with article 28 may be achieved with measures that are not included in the Guidelines and compliance with the Guidelines alone does not guarantee full legal compliance with the DSA.

Some of the key provisions are:

- a) Two **key principles** guide the provisions: (i) risk-based approach, building on the example of the risk assessment and mitigation obligations of article 34 & 35; (ii) a rights-based approach that contemplates children's rights to protection, privacy, non-discrimination, freedom of expression and participation equally.
- b) **Age Assurance**: online platforms must implement age assurance methods that are accurate, reliable, robust, non-intrusive and non-discriminatory. The recommendations follow a risk-based approach:
 - For services that provide adult content (i.e., pornography or gambling) or which are restricted to a legal age of access by national law, the Guidelines recommend the use of age verification tools.
 - For other services, such as when Terms & Conditions prescribe a minimum age of access – i.e., 13 for social media –, the guidelines recommend age estimation. This does not exempt the online platform from putting in place other measures to protect children.
 - In any case, the Guidelines consider that self-declaration of age is not a suitable method.
- c) **Account settings** – the Guidelines recommend that online platforms include private by default settings for children, and that features that increase risk of harm — such as download or screenshot ability of minors' content, ability to add children to groups or addictive design — are disabled by default. The guidelines also recommend to ensure that children are provided with incremental degrees of control over such settings according to their age and evolving capacities.
- d) **Online interface design** – the Guidelines recommend that providers disable features that predominantly encourage engagement and implement functionalities allowing minors how to engage with their services, including time management tools, reporting tools, options to disable AI features, among others.
- e) **Recommender systems** – the Guidelines recommend that platforms prioritise content recommended on the basis of explicit user signals (i.e., *like, don't show me more* buttons) over behavioral signals (i.e., stop the scrolling to watch or spend more time watching one video over another one) for minors. We believe this is a missed opportunity to prohibit content recommendations based on the behavioral profiling of children.
- f) **Commercial practices** – the Guidelines reinforce that children's lack of commercial literacy should not be exploited in any way, especially recommending that children are not exposed to

- Harmful or excessive advertisement, that AI systems do not nudge children towards commercial content and ensure that commercial content is properly labelled.
- Practices that can lead to excessive spending – including by communicating the value of economic transactions transparently (i.e., virtual currencies or free games with in-game purchases) and avoiding the exposure to gambling-like features including loot boxes.

g) **Content moderation** – the Guidelines encourage platforms to

- Ensure effective content moderation, including setting robust moderation policies and putting in place effective moderation technology and trained human moderators, operational in all the official language(s) of the country.
- Implement safeguards that prevent AI systems from generating harmful content for children.
- Provide options for children to block or mute users and ensure they cannot be added to groups without explicit consent. These are aimed to help reduce risks of cyber-bullying, harassment or grooming.
- Transparently report on the effectiveness of their content moderation practices, including the prevalence of harmful content and conduct.

h) **Reporting tools and user support measures** – provide child-friendly user reporting, feedback and complaint tools and ensure platforms respond promptly to reports made by children. Platforms should also put in place information and facilitate access to support service (i.e., helplines and hotlines) to children who encounter harmful content or conduct.

i) **Tools for guardians** – the Guidelines recommend platforms put in place age-appropriate and child-rights respecting (including privacy and access) parental control tools.

j) **Child participation in governance** – children should be given meaningful opportunities to participate in design, governance and decision-making that affect them (for example, via consultation, feedback loops).

Key considerations for national implementation

The DSA, as an EU regulation, has direct legal force across all Member States. Because the Guidelines are EU-level and non-binding, their impact depends strongly on national implementation, enforcement and oversight. They provide the European Commission’s official interpretation of how Article 28 (“protection of minors on online platforms”) should be applied in practice, acting as **soft law** or interpretative guidance — helping platforms, regulators, and courts understand how to comply with the DSA’s existing legal requirements.

Therefore, **compliance with the Guidelines alone does not guarantee full legal compliance** with the DSA. This is because the Guidelines provisions illustrate good practices or examples

of how Article 28 obligations might be met, but they do not substitute for the regulation's mandatory duties and thus online platforms can still fail to comply with other provisions of the DSA.

Secondly, the DSA requires platforms to take *appropriate and proportionate* measures to ensure a high level of protection for minors. As this will depend heavily on factors such as the platform's size, nature, and risk profile, even if a platform follows the Guidelines generally, regulators may still find that its measures are inadequate given the specific risks of its service.

Third, the Guidelines represent a "snapshot" of current best practice, but as the digital environment evolves, platforms will still need to update their measures to reflect future DSA enforcement decisions, delegated acts, or case law.

While the enforcement of the DSA provisions with regards to big online platforms falls on the European Commission, the application of these provisions for the rest of online platforms falls on the national regulator of the country where the online platform is based.

Such regulator – designated "Digital Services Coordinator" – is appointed by national governments and should watch out how online platforms actions are in compliance with the Guidelines provisions outlined above. They should take the Guidelines provisions as reference when issuing enforcement decisions or supervisory guidance. Each Member State's Digital Services Coordinator has discretion in assessing whether a platform's measures meet DSA standards.

This means that although the Guidelines set a common reference across the EU, Member States must ensure that national laws, regulatory frameworks and sector-specific rules (e.g., on age verification, gambling, pornography, media services) are aligned with the Guidelines. However, Coordinators may also interpret the DSA Guidelines more strictly or apply additional national requirements (e.g., stricter age-verification rules).

In enforcement or litigation, regulators and courts will use the DSA's legal text as their primary reference. They may draw on the Guidelines as persuasive evidence of good practice, but they are *not obliged* to accept compliance with the Guidelines as proof of full legal compliance. In some cases, failure to go *beyond* the Guidelines — where risks to children are significant — could still be judged insufficient.

As a result, **compliance with the Guidelines does not equate to compliance with the DSA**. Full compliance requires satisfying both the DSA's binding legal obligations and any national implementation measures — not just adherence to the Commission's recommendations.

Some additional challenges remain for the national implementation of the DSA:

- Cross-border issues: some platforms who are not considered VLOPs or VLOSEs operate across borders, requiring coordination among national regulators of different countries. The Digital Services Board brings together regulators from different countries, offering a space for such coordination.

- Platform size issues: while the DSA and the Guidelines exempt micro and very small enterprises, many smaller platforms still pose risks to children and national regulators should find ways to encourage platforms of smaller scale to meet appropriate standards.
- Digital Services Coordinators across the EU have different levels of capacity – both in terms of resources and legal powers – to properly enforce the DSA Guidelines.
- Effectiveness: as seen in the previous round of risk assessments submitted by VLOPs under the DSA, many of these tools do not translate in effective safety for children even once implemented. For example, while online platforms claim to have age-appropriate reporting tools, children continue to portray them as difficult to use and report lack of action by the platforms. In many cases, this is a matter of unequal deployment across Member States or insufficiently reaching children at risk.

What does this mean for Child-Rights Organisations?

Child-rights organisations can monitor whether platforms accessible to minors in their country comply with the measures recommended by the Guidelines. Its provisions offer therefore **advocacy leverage** for child rights organisations to push national regulators and governments to hold platforms accountable when there are breaches of online child safety in their services.

Civil Society can monitor the implementation of the Guidelines in many ways. For instance, they can help identify which online services are accessible to minors, and whether they fall under the DSA/guidelines and benchmark platform practices against the Guidelines, identifying whether key recommended measures are visible and effective. This evidence can be relevant for regulators, especially in those countries where less resources have been allocated to them.

Child rights organisations can also leverage the guidelines to push regulators to prioritise the protection of minors online and promote child participation both in policy-making and in platform design. Finally, it is crucial they empower children, parents and caregivers to understand their rights under the DSA and the protections offered by the Guidelines.

By becoming Trusted Flaggers¹, certain child rights organisations can contribute to the implementation of some Guidelines provisions more directly. For example, the Guidelines recommend platforms to prioritise reports that concern the privacy, safety and security of minors with appropriate response times – without prejudice to the priority status already granted by Article 22 of the DSA to reports coming from Trusted Flaggers. The guidelines also encourage platforms to collaborate with other trusted flaggers – among other stakeholders – to identify good technological solutions to ensure a high level of privacy, safety and security for children.

¹ Trusted flaggers are entities with particular expertise and competence in detecting certain types of illegal content, and the notices they submit within their designated area of expertise must be given priority and processed by providers of online platforms without undue delay. They are appointed by the DSC of the Member State where the entity is established.

Conclusion

The Guidelines on the protection of minors under the DSA represent a significant step forward in providing a standard for how online platforms should protect children's rights in the digital environment. For child-rights organisations, they offer an important tool: a benchmark for advocacy, monitoring and national implementation efforts.

However, much will depend on how effectively national regulators implement, supervise and enforce these provisions — and whether platforms translate recommendations into meaningful change.

Further reading

[Guidelines on the Protection of Minors Online](#)

Eurochild, [Recent updates on EU Digital Policy, a closer look to the Digital Services Act, 2024](#)

5 Rights, [Analysis of the Guidelines to Article 28.1 of the Digital Services Act, 2025](#)

ANNEX I. List of National Digital Coordinators

Belgium: Belgian Institute for postal Services and Telecommunications

- Contact details: info@bipt.be

Croatia: [Hackom](#)

- Contact details:
Legal and natural persons: pisarnica@hakov.hr
State institutions and public law bodies: e-pisarnica@hakov.hr

Cyprus: Radiotelevision & Digital Services Authority

- Contact details: crtauthority@crt.a.org.cy

Denmark: Agency for Digital Government

- Contact details: digst@digst.dk

Estonia: Consumer Protection and Technical Regulatory Authority

- Contact details: info@ttja.ee

Finland: Traficom

- Contact information: [Yhteystiedot | Traficom](#)

Germany: Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railways

- Contact information: [Bundesnetzagentur - Contact](#)

Greece: Hellenic Telecommunications and Post Commission

- Contact details: info@eett.gr

Hungary: National Media and Infocommunications Authority

- Contact details: info@nmhh.hu

Ireland: Media Commission

- Contact details:
Contact centre: usersupport@cnam.ie
Corporate head office: info@cnam.ie

Italy: Agcom

- Contact details:
Email: info@agcom.it
PEC: agcom@cert.agcom.it

Lithuania: Communications Regulatory Authority

- Contact details: rrt@rrt.lt

Malta: Malta Communications Authority

- Contact form: [Contact | MCA](#)

Netherlands: Authority for Consumers and Markets

- Contact details: acm-post@acm.nl

Portugal: National Communications Authority

- Contact details: info@anacom.pt

Slovenia: Agency for Communication Networks and Services of the Republic of Slovenia

- Contact details: info.box@akos-rs.si

Sweden: Post and Telecom Authority

- Contact details: pts@pts.se

For more information, contact:

Francesca Pisanu

EU Advocacy Officer

Francesca.pisanu@eurochild.org

Eurochild AISBL

Avenue des Arts 7/8, 1210 Brussels

Tel. +32 (0)2 511 70 83

info@eurochild.org – www.eurochild.org

© Eurochild 2025

