5RIGHTS FOUNDATION

31 October 2025

Guidelines 3/2025 on the interplay between the DSA and the GDPR

Response to the European Data Protection Board's Consultation

Overview

The 5Rights Foundation welcomes the opportunity to comment on the draft guidelines on the interplay between the Digital Services Act (DSA) and the General Data Protection Directive (GDPR). The rights of the child, as established by the UN Convention on the Rights of the Child and elaborated as regards the digital environment in UNCRC General comment No. 25, must be a key element informing the implementation and application of these legislation and their interplay. This document outlines 5Rights' key considerations and input on how the DSA and the GDPR can ensure the respect of the rights of the child in the digital environment.

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

1. General comments

We welcome the EDPB guidelines as they further clarify and specify the interplay between two essential pieces of legislation regulating the online environment, the DSA and the GDPR. We strongly believe that those legal frameworks should reinforce each other in ensuring the respect of children's rights. The GDPR recognised the vulnerabilities of children in the digital environment and called for additional protection. Grounded in its principles and informing its implementation, several national authorities adopted guidelines to further detail how children's data should be protected, including:

- CNIL Recommendations on the Digital Rights of Children
- Irish Fundamentals for a child oriented approach to data processing
- Dutch Code for Children's Rights
- Swedish Rights of Children and Young People on Digital Platforms

The DSA complements this framework by providing for a general requirement to ensure children's privacy, safety and security on online platforms and prohibits targeted advertisements for children based on their personal data. The guidelines adopted in July 2025 by the European Commission provides additional details and guidance in regards as to the measures and processes required to ensure a high level of privacy, safety and security. In those guidelines, the European Commission adopted a child mainstreaming perspective. To ensure a high level of privacy, safety and security, they recognise that several obligations under the DSA must be interpreted from a children's rights perspectives – including on issues such as dark patterns, profiling and recommender systems. That approach could be strengthened in the current draft guidelines whose focus on children is limited if not absent in certain key chapters.

In implementing both those legislations and clarifying their interplay, **children's rights must remain central.** The guidelines proposed by the EDPB must therefore be strongly grounded in children's rights and fundamental rights. Indeed, the DSA aims to ensure a "safe, predictable and trustworthy online environment in which fundamental rights are protected". The GDPR aims to protect fundamental rights, and in particular the right to the protection of personal data. In both legislation, children are recognised as a group that deserves additional protection (recital 38 GDPR). In its executive summary, the EDPB mentions privacy and protection of all users as to be balanced against the safety and security of minors. It is important to note in that context that children also have a right to privacy and that in all decisions concerning children, their best interests must be the primary consideration (article 3 UNCRC).

Currently, the guidelines **fail to highlight the complementarity of both legislation in furthering a safe online environment** for children and focus rather on one specific measure, namely age assurance. This is problematic as data protection principles do more than limit the use of age assurance, but are overall critical in ensuring children's privacy online. The chapter on the protection of minors must be significantly revisited based on a more comprehensive understanding of the risks that children face online and on the interplay between the two legislations as to how they address those risks.

We do believe the guidelines are critical both in terms of compliance from the private sector but also in terms of implementation and enforcement. To ensure that children's rights are respected throughout the online environment, national and European authorities **must be consistent** and ensure the same level of fundamental rights protection everywhere. In addition to the guidelines, cooperation and coordination amongst relevant authorities on a regular basis is necessary to further that coherence and consistency in practice.

Finally, as presented in the EDPB's work programme 2024-2025, we would strongly support the **adoption of guidelines on children's data**. In view of the interplay between the DSA and the GDPR, those guidelines appear increasingly necessary as data protection underpins privacy, safety and security for children online.

2. Protection of minors

We would like to underline that the protection of minors online, ensuring a high level of privacy, safety and security for them, requires a robust implementation and enforcement of data protection rules. This should be highlighted within section 2.6.

As noted earlier, the two legislations are complementary in this regard as is demonstrated by the different DPA's guidelines cited in the European Commission guidelines on article 28.

However, para 90 seems to be implying that the most risks in terms of the protection of minors come from companies putting in place measures to ensure a high level of privacy, safety and security that will in turn lead to data protection risks. While it is true that any measures put in place for the protection of minors must respect data protection rules, it is far from sufficient to limit the understanding of GDPR-DSA interplay in terms of minors' protection to one of potential conflict rather than complementarity. The most risk to privacy of children is not in the way that measures are taken to implement article 28.1 but rather in the misuse and exploitation of their data in the first place.

Indeed, **many risks faced by children online are directly linked to the processing of their personal data, as recognised under recital 75 GDPR**. The EDPB should emphasise that to ensure a high level of privacy, safety and security, companies must strictly comply with existing legislation, notably the GDPR. This is especially crucial as 'privacy' is directly mentioned in Article 28(1) – recognising that it is a key and central risk that children face online. It should be recognised that privacy is an enabling right supporting children's ability to enjoy their other fundamental rights. The current draft should highlight the data protection risks faced by minors online and **should make clear that ensuring compliance with the GDPR goes hands in hands with ensuring a high level of privacy safety and security under the DSA.** For instance, the right to be forgotten is particularly useful for children as they might be unaware of the risks of sharing certain content or information online or that content might have been shared without their consent (recital 65 GDPR). This information might prove to undermine their safety in some cases and/or their privacy. Measures relating to recommender systems also touch upon both safety and privacy, as children's personal data might be used to personalise feeds which in turn may lead to rabbit holes effects and harmful content. It is critical to ensure that children's data is not repurposed to exploit their vulnerabilities. The guidelines should therefore underline how the DSA and the GDPR complement each other to ensure safe children's online experiences and the protection of their data.

Certain measures, such as transparency under both legislations, do reinforce each other and clearly require companies to ensure that information provided to minors are accessible and easily understandable (Article 12 GDPR, see point 8.4 Guidelines on the protection of minors, Article 14,15 and 24 DSA).

Regarding **age assurance**, we support the recognition of the risks that such systems may pose to the personal data of children and underlining that they must be in line with the GDPR. However, the current guidelines should not limit their understanding to age assurance as a method of age restriction rather than as a means to provide for a safe and age-appropriate experience online. Many of the guidelines by DPAs on the topic do note the necessity of age assurance measures, especially in relation to consent of processing of personal data under Article 8 GDPR.

We would also like to note that the sentence in §91 is confusing: "Moreover, from the perspective of EU data protection law, providers of online platforms should ensure a high level of privacy, safety and security for all its users (not only minors)". The DSA requires explicitly for online platforms to ensure a high level of privacy, safety and security for minors. While both the DSA and the GDPR aims to ensure the fulfilment of the fundamental rights for all, both legislations do recognise that children need additional safeguards and protection. Ensuring an overall safe online environment will inevitably benefit children, children's specific vulnerabilities should however still be considered rather than ignored.

3. Governance and enforcement

We welcome the focus on cooperation and coordination amongst authorities to ensure a consistent application of the legislations in line with the principle of sincere cooperation. In cases, where the Data Protection Authorities have been designated as competent authorities, cooperation mechanisms and regular exchanges at national level should indeed be actively encouraged (para 115). Such dialogue should also be explicitly encouraged between the Commission and data protection supervisory authorities within para 117.