



Universiteit
Leiden
The Netherlands

Submission on the European Commission Art. 28 draft guidelines

Hof, S. van der

Citation

Hof, S. van der. (2025). *Submission on the European Commission Art. 28 draft guidelines*. Leiden. Retrieved from <https://hdl.handle.net/1887/4273599>

Version: Accepted Manuscript

License: [Licensed under Article 25fa Copyright Act/Law \(Amendment Taverne\)](#)

Downloaded from: <https://hdl.handle.net/1887/4273599>

Note: To cite this publication please use the final published version (if applicable).

Submission on the European Commission Art. 28 Guidelines

Professor S. (Simone) van der Hof ~ Professor of Law and Digital Technologies, Center for Law and Digital Technologies (eLaw), Leiden Law School, Leiden University

12 June 2025

The Guidelines are a very welcome interpretation of the high level of protection of the privacy, safety and security of minors in Article 28 of the DSA. The Guidelines provide important guidance on the design of services appropriate, or at least not harmful, for minors. It is greatly appreciated that the lived experiences, expectations, and views of children and young people have been and will continue to be considered in the drafting of these Guidelines. On a few points, the Guidelines could clarify or strengthen the instructions for online platforms. This submission will focus on the following topics: (a) Risk-based approach, (b) Age assurance, (c) Illegal and harmful content, (d) Commercial practices, and (e) AI and chatbots.

(a) Risk-based approach

The Guidelines appear to advocate a risk-based approach with references to medium and high risk (and presumably low risk, although that term is not used). However, it is not clear from the Guidelines when a practice should be classified as low, medium or high risk. With a risk-based approach, it is essential that the Guidelines provide **more clarity on the interpretation of these risk levels** because the choice of what are considered adequate and effective preventive or mitigating measures (e.g. the level of age assurance) depends on this. Inspiration can e.g. be drawn from scientific research and related legislation. In the latter case, it is relevant, for example, that the processing of children's personal data under the GDPR is considered high-risk processing, for which there is a higher threshold with regard to the principles of fairness, lawfulness and transparency. Similarly, e.g., guidance from the AI Act on prohibited or high risks AI systems or practices is relevant in terms of risk levels indicated by the Guidelines.

Furthermore, it is important to explain the relationship between Article 28 DSA and Articles 34 and 35 of the DSA in this context more explicitly than is currently done in the Guidelines, as the provisions are all relevant to the protection of minors and the protection and respect of children's rights, which means that they overlap and complement each other in relation to the risks that online platforms must address. In that respect, it is important to know **how systemic risks relate to the low, medium and high risks levels** addressed in the Guidelines. It seems appropriate to explicitly state that systemic risks to the protection of minors are high risks and that risks other than systemic risks may be high risks depending on the situation.

Moreover, it is essential for the adequate implementation and assessment of a risk-based approach under Art. 28 DSA that there is a **clear methodology** that online platforms can use **for impact assessments**. It is appropriate to align with existing impact assessments as the Guidelines do, and the Commission's announcement to provide additional guidance is

wholeheartedly supported. Additionally, a requirement for the involvement of children and **child-friendly versions** of impact assessments can be made explicit in the Guidelines. Once again, it is important to ensure proper coordination between the Article 34 DSA risk assessment and the Article 28 DSA impact assessment. In the latter case, the impact should be broader than the potential risks posed by online platforms to the rights and well-being of children, and **consideration** should also be **given to the positive impact on their rights and well-being**. In this context, greater emphasis should be placed on the **proportionality of measures** regarding measures that respect all children's rights, i.e. children's participation, protection and provision rights. In addition, **metrics** for the effectiveness of preventive or mitigating measures should be provided and implemented to better assess the extent to which they have the desired or required effect on the protection of children's privacy, safety and security.

Finally, given the **relevance of the precautionary principle** in children's rights (see, among others, GC25), it is important that the Guidelines relate to that principle in relation to a risk-based approach to ensure the safety of children. This means that where we have reasonable indications that a particular practice or design choice poses risks to children, precautionary measures should be taken (ideally by not applying the practice or design choice to children), even if there is **no conclusive evidence** that its effects are harmful to (groups of) children. This is necessary because research into possible harmful effects to the rights and wellbeing of children takes (a lot of) time and resources, and research involving children presents challenges, while the impact may already be felt.

(b) Age Assurance

The focus on age assurance as a necessary or preventive measure is to be welcomed. However, the **distinction between** the general terms and conditions of online platforms that apply a **minimum age of 18** and those with a **lower minimum age is unjustified**. In both cases – the platform is unsafe or unsuitable for children under the minimum age – age verification is, in principle, the necessary measure. It is inexplicable why children are adequately protected in one case and in another case are dependent on a system (age estimation) that is less reliable. In both cases, age estimation may still be adequate if the online platform indicates that the minimum age is based on reasons other than ensuring the safety of children, but this should not depend on the minimum age (18 or younger).

Moreover, **important examples of legal requirements for age verification** are **not mentioned**, such as the legal capacity of children to enter into agreements or give consent to online platforms for the processing of their personal data. The minimum age for legal capacity is laid down in the national legislation of EU Member States, and online platforms must take this into account for the lawful contracting and processing of personal data. Furthermore, the text of the Guidelines now suggests that the minimum age for legal capacity (or access to services or content) is always 18 years, but this is not necessarily the case. **Age verification solutions must therefore be accessible to children of all ages**, and this is currently not or insufficiently recognised in the Guidelines.

Furthermore, it is good that the Guidelines indicate that self-declaration is not an adequate method of age assurance. However, this conclusion also applies – for other reasons – to

another method used, namely behavioural profiling as age assurance. Behavioural profiling as age assurance is unlikely to comply with the GDPR and is a high-risk AI system (i.e. a biometric categorization AI system) under the AI Act. Although the Guidelines may apply (based on the EDPB statement on age assurance) that **behavioural profiling as age assurance is not an adequate method**, the text can be clearer. An academic article is expected to be published on this topic: MR Shaffique, S van der Hof, 'Behavioural Profiling for Age Assurance: Do The Ends Justify The Means?' (under review).

Similarly, line 305-306 ("one verification and one estimation method should be provided") should be formulated differently so that it is clear that there must be a **choice of age assurance methods** for users of digital services, but that in the case where age verification is required, one of those methods cannot be age estimation. The text as it is currently worded is confusing in that regard. A choice of age assurance methods and service providers is potentially compromised and dependence on non-European solutions is increased with the option of age assurance in operating systems, and it is not advisable to mention this as an example in the Guidelines (lines 361-362).

(c) Illegal and harmful content

The Guidelines do not sufficiently distinguish between illegal and harmful content. From the perspective of **protecting the freedom of information and expression rights of users** of online platforms (inclusive), it is **essential to make the distinction between illegal content and harmful content very clear. Illegal content must be removed for all users** (and therefore not only for children, even though they may be more vulnerable). The DSA does not define what constitutes illegal content (this is determined by the national legislation of EU Member States), but it does specify the **process for the removal of illegal content** by intermediary services (Chapter II DSA) which can be claimed, must be **understandable and easily accessible to children** in accordance with Art. 28, preferably, removal of illegal content should be achieved **through easily recognizable uniform procedures** across the EU. Trusted flaggers can play an important role in ensuring children's access to these procedures, advising them on illegal content and the safe use of online platforms.

Harmful content is content that may be harmful to the development of children. This content **does not need to be removed from online platforms**, but children do deserve protection from harmful content by not being (unexpectedly) confronted by it. Harmful content is therefore directly covered by the protection of children's safety as also regulated in Article 28 of the DSA. To protect children from harmful content, a **distinction** is made by the AVMSD, regarding video sharing platforms, **between (1) the most harmful content** (e.g. extreme violence and pornography) **and (2) other harmful content**. First, **for the most harmful content** the most stringent measures must be taken (Article 28 bis AVMSD). This means that children must be kept away from this content and the **most effective measure is age verification**. The minimum age for access to the most harmful content is determined by the EU Member States and may be, for example, 16+ or 18+. Second, **children should not be unexpectedly confronted with other harmful content** that is not the most harmful content. This can be achieved by providing content with a content and age rating developed on a scientific basis. The content rating can include traditionally

harmful content such as violent, scary, discriminatory or sexually explicit content (to the extent not already covered by the most harmful content), but also **new forms of harmful content**, such as challenges and unhealthy information.

Moreover, it is recommended that the Guidelines align with the AVMSD by not merely proposing one measure (content moderation) but leaving room for and recommending other, evidence-based and potentially more adequate and effective, measures and ensuring that children and parents are empowered to make choices appropriate to the age of the child. Preferably, **uniform measures** should be adopted across the European Union so that they are easily recognizable by children and parents. One possibility is to provide **creators** on platforms with a **functionality** (and related guidance and education) that supports them in adding **content and age ratings to the content** they create and share on the platform (to the extent the content is potentially harmful for children). This allows children (and guardians) to make informed choices about whether to view certain content, as they are told why certain content may be harmful. Simply blurring content, for example, is insufficient if you do not know why the content has been blurred and can be counterproductive if it makes children curious. With content ratings, content can also be automatically filtered based on parameters set in advance by guardians or children and it is recommended that online platforms provide such features if they do not yet have them.

(d) Commercial practices

The Guidelines mention the prohibition of behavioural advertising in Art. 28(2) DSA; however, they pay little attention to the online (behavioural) profiling of children for commercial purposes, other than behavioural advertising. In line with both the UN CRC General Comment 25 and the Council of Europe Recommendation CM/Rec(2018)7, it is relevant that the Guidelines indicate that **online commercial profiling of children** is, in principle, **contrary to the high level of privacy (and safety) that children deserve under Article 28 DSA**, as well as the GDPR, in accordance with its Recitals 38 and 71. It is recommended that the combination of consumer, privacy and advanced technology risks also include the online profiling of children for commercial purposes. For further reading on online commercial profiling of children (including a children's rights and legal analysis): EL Leijten and S van der Hof, '[Dissecting the Commercial Profiling of Children: A Proposed Taxonomy and Assessment of the GDPR, UCPD, DSA and AI Act in Light of the Precautionary Principle](#)' (2025) 57 Computer Law & Security Review.

Specifically with regard to recommender systems, the text of the Guidelines could be tightened up by clarifying that behavioural profiling (e.g., line 535-536 - delete the strikethrough words: "the ~~ongoing~~ collection of behavioural data"), engagement-driven design (e.g., lines 529-530 - delete the strikethrough words: not ~~only~~ optimising or ~~predominantly~~ maximising time spent on"), and exposure to content that poses risks to children (e.g., line 551 - delete the strikethrough words: "prevent a minor's ~~repeated~~ exposure") are design choices that are not in accordance with Art. 28 DSA. The **default should be a recommender system that is not based on online (behavioural) profiling of children**. Instead, children should be given the option to easily choose their own parameters for personalizing content. An important starting point should also be that children receive a **diversity of age-appropriate content** in accordance with Art. 17 UN

CRC. A recommender system should preferably surprise children in a positive way by stimulating their curiosity with age-appropriate content that shows them something new (for example, via a 'surprise me' button or automatically).

e) AI and chatbots

Online platforms are increasingly implementing AI practices, including chatbots, in their services used by or impacting children. **AI practices and chatbots** can pose significant risks to children's privacy, safety and security. These developments **deserve much more attention in the Guidelines** by indicating what measures are needed to protect children or draw red lines where these practices (or services offering them) cannot be safely offered to children. If there are indications of unsafe practices, the **precautionary principle**, again, requires (as also acknowledged by UN CRC General Comment 25 and the AI Act) that the safety of children be paramount and that certain services or functionalities be restricted for children by implementing age verification.

In this context, it is essential that the Art. 28 DSA Guidelines are **aligned with other relevant legislation such as the GDPR and the EU AI Act**. The Guidelines should take into account, for example, the prohibited practices in Art. 5 AI Act that specifically target and exploit the vulnerabilities of children (and refer to Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)), as well as high-risk AI systems that may also have an impact on children (see earlier in this Submission on behavioural profiling for age assurance) (and refer to Guidelines on the regulation of these systems once they are published).