ministry of digital affairs

Case no.
2025 - 2150

Document no.
143397

Date
13/06/2025

The Danish government's response to the Commissions consultation regarding Article 28 of the Digital Services Act

The Danish Government would like to express its appreciation for the chance to respond to this consultation. Protecting minors online is a key priority of the Danish government to which strong enforcement and effective implementation of the DSA is pivotal. Article 28(1) is the heart of the DSA's approach to the protection of minors on online platforms, and accordingly, the guidelines will be central in ensuring the effective enforcement of article 28 in all Member States.

The Danish Government welcomes the Commission's draft guidelines, which hold great potential to improve the privacy, safety and security for minors online. However, in order for the guidelines to have the desired effect and realize their potential, it is crucial that online platforms and especially social media correctly identify and categorize their users as being minors or not. Unfortunately, the draft guidelines fall short of this objective.

The draft guidelines' proposed approach of relying primarily on age *estimation* for major social media platforms is insufficient given the comprehensive risks these platforms can pose to minors and given their documented ineptitude at keeping minors from their service using other age estimation techniques. The Danish Government finds it to be of utmost importance that the guidelines are amended to require availability of robust age *verification* mechanisms as the default standard for all platforms, presenting a wider range of risk categories to minors.

In the following, we elaborate our key messages regarding the draft guidelines:

- Clear recommendations on effective and privacy-preserving age verification;
- A broad scope which covers all platforms that are actually accessible to minors;
- Welcoming the risk-based approach, but social media platforms should be categorized as high risk per default;
- Ensure that minors are not exposed to retention mechanisms and addictive designs and make use of default settings to ensure a baseline of safety for minors;
- AI Chatbots should be disabled by default, not require payment to opt out of and be free of manipulative designs;
- Making it as easy to report illegal and harmful content as it currently is to "like" or "share" content.

Clear recommendations on effective and privacy-preserving age verification

The guidelines should make it crystal clear that all relevant online platforms and especially social media should implement age verification to comply with Article 28 of the DSA.

If providers are to ensure safe and secure platforms with age-appropriate content and interfaces, the provider must have a firm awareness of the age and maturity level of their users. Effective age verification is a prerequisite for this. That is made abundantly clear, as the major social media platforms use age estimation techniques, but still fail to keep children below their own age limits from their services. A study from 2024 shows that 48 percent of all Danish children have a profile on social media before they turn 10 years old, whereas 94 percent have a social media profile before the age of 13. This is despite the fact that major social media platforms by their own accounts use 'effective' age estimation and typically do not allow children below the age of 13 on their platforms.

The draft guidelines' proposed approach of relying primarily on age estimation for major social media platforms is insufficient given the comprehensive risks these platforms can pose to minors. Many online services and platforms can be harmful for minors if accessed without guardrails and protections. Therefore, efficient age verification tools are needed in order to protect minors in digital environments. Such tools are under rapid development, and will soon be available across many EU member states.

Age estimation techniques have significant accuracy limitations, with error rates that may be hard to prove or investigate, and with a lack of transparency in terms of their application. Additionally, such estimation techniques may be opaque and very data-intensive in terms of analysis of user behavior, and may sometimes be bordering on profiling of users.

Age verification may introduce a small friction for users. However, it is a proportionate measure to protect minors from the risks (content, conduct, contact, consumer, cross-sector) on many online platforms. In the offline world, age checks are standard for age-restricted goods and services. Thus, it is perfectly reasonable to expect similar safeguards online, where the risks — especially for children and teens — are significant and well-documented.

Against this background, the Danish Government strongly recommends that the draft guidelines are amended to require availability of robust age verification mechanisms as the default standard for all platforms, presenting a wider range of risk categories to minors. Specifically:

- Online platforms and especially social media should be required to enable and implement age verification relying on the technical specifications used in the forthcoming EU age verification app and EUDI Wallet.
- The guidelines should establish clear criteria for when alternative approaches may be permitted, with the burden of proof resting on the platforms to demonstrate the efficacy of less stringent measures.

The guidelines envision an EU age verification app primarily targeted at 18+ restricted content like pornography and gambling. The Danish Government suggests, that the guidelines make it clear, that where more granular age-verification is available, all relevant online platforms and especially social media should make use of these.

The Danish Government believes that the upcoming EU age verification app and the European Digital Identity (EUDI) Wallet will provide a commonly available, seamless and privacy-preserving way to verify age, which will minimize friction especially if the verification method is broadly adopted, and thus familiar to the user. While some member states may not be able to issue +13 or +15 age attestations, many member states are in fact able to do so, or will be able to do so in the future. Protecting minors online using age verification in these member states should not be limited by the fact that other member states do not have such technical solutions ready. Especially since it will not substantially increase the technical complexity for service providers to utilize the age verification solutions.

Please find our proposed concrete changes to the draft guidelines regarding age verification in the annex.

A broad scope which covers all platforms that are actually accessible to minors

In order to ensure the same level of protection for all minors in the EU, it is essential that all online platforms where children are present, adhere to the guidelines. Hence, we appreciate how the Commission has sought to further clarify which online platforms are obligated to comply with Article 28. We welcome that it is expressed clearly that also online platforms which state in the terms and conditions that the platform is restricted to users above 18 years of age, shall comply with the guidelines where users under the age of 18 in fact use their services.

However, the interpretation of how providers can become aware of the fact that some recipients on their services are minors, could be improved. As currently phrased, the examples are limited to situations where the provider processes relevant personal data or has conducted or commissioned its own research on whether minors access their platforms. This does not consider information from external sources, including academic studies, civil society organizations and regulatory bodies, which often document widespread use of platforms by minors. In several instances, this type of evidence has been publicly available without being acknowledged or acted upon by platform providers. We therefore recommend that the guidelines clarify that a platform is also considered to be aware of minors accessing its services, where independent and credible third-party evidence points to the presence of minors on that platform.

Following a risk-based approach to the protection of minors, but social media platforms should be categorized as high risk per default

The Danish Government welcomes how the draft guidelines adopt a risk-based approach, recognizing that different platforms pose varying levels of risk to minors. Accordingly, the draft guidelines recommend that each platform tailor their measures to their specific services. While we agree with this approach, it should be redundantly clear, that all social media platforms covered by Article 28 of the DSA are considered a high-risk category and that they must adhere to the highest standards set out in these guidelines.

Social media platforms pose significant risks to minors. They entail a juxtaposition of functions posing a variety of risks to their users, including exposure to harmful content, addictive designs, commercial profiling, and retention mechanisms, harmful encounters with adult predators, and many more. As a result, European children are too often exposed to illegal or harmful content and comments, and faced with unwanted contacts online. Social media algorithms push extreme content to vulnerable minors, which can cause or exacerbate mental health problems, including self-harm, poor body image or eating disorders. Recent years have seen a sharp rise in problematic social media use among minors in Europe, spurred by retention mechanisms intentionally designed to catch and keep minors' attention. Such problematic social media use can cause addiction-like symptoms, lower mental and social well-being and is even correlated with higher substance use. The guidelines must ensure that social media platforms understand that they carry the responsibility to reverse this development.

In addition, a risk-based approach should take into account that many online platforms have mixed target groups and users. This entails outlining clear and practical definitions of what constitutes inappropriate content for minors and how the particular type of content should be categorized based on its harmful nature, in order to help the individual industries to identify and mitigate risks.

The annex included with the draft guidelines, presenting the OECD 5C typology of risks, are hence not only useful, but necessary. While we can support the use of the OECD typology, we nevertheless find that it would prove useful for implementation and enforcement purposes to include further examples of the different risk categories. Most pressingly, the Danish Government would urge the Commission to include content promoting "self-harm" among the examples of "Content risks". Studies show that more than 21 percent of Danish children in the

ninth grade have committed self-harm. The sharing and promotion of self-harm content on social media is a recurring problem, that needs to be addressed.

Ensure that minors are not exposed to retention mechanisms and addictive designs and make use of default settings to ensure a baseline of safety for minors

Default settings can play a crucial role in protecting minors online by offering a baseline of safety without requiring a proactive effort from the minor. The Danish Government hence welcomes how the draft guidelines recommend implementing default settings which create a consistent layer of protection. We further support how the draft guidelines allow for parental control mechanisms, but at the same time recommends default settings ensuring that even less tech-savvy families benefit from safety measures, reducing the chances of minors being accidentally exposed to risks.

We also appreciate that the Commission has responded to our call for an exhaustive description of useful and recommended default settings, including time notifications, turning off "geolocation", "seen" and "read" function and the recommendation to make some functions less visible, e.g. the "like" function.

Of particular importance is to ensure that minors are never exposed to retention mechanisms and addictive designs when engaging on online platforms. For this reason, it is central to maintain the recommendation on online interface design in the draft guidelines, which state that online platforms should ensure *"that minors are not exposed to persuasive design features that are aimed predominately at engagement or that may lead to extensive use or overuse of the platform or the forming of problematic or compulsive behavioural habits"*, as well as maintain the useful examples of such design features, including "infinite scroll" and "auto play".

AI Chatbots should be disabled by default, not require payment to opt out of and be free of manipulative design

The Danish Government appreciates that the draft guidelines acknowledge the specific risks posed by AI systems such as chatbots and filters, including the need to clearly inform minors when they are interacting with non-human agents. However, transparency is not enough to protect children from the risks posed by AI-chatbots, and it should not be the children's responsibility to ensure that online platforms are safe environments for them to engage in.

Certain AI-chatbots have been shown to emotionally manipulate with children and create a false sense of safety and relational closeness. They have further ended chats with suggestions for the child to "share more", noting that the chatbot is "there for them". This kind of emotional engagement retains children on the platform and increase their dependency of it.

We therefore urge that the guidelines recommend that AI-chatbots are disabled by default and that they should be free of manipulative design. Minors should not be locked into interactions with a chatbot which can influence their behavioural, buying and spending patterns. Some online platforms require that users pay for removing the AI-chatbot once installed, why it should be made clear that such practice is unacceptable. Minors should always be able to remove AI-chatbots free of charge.

We further recommend that the guidelines emphasize that AI chatbots must be designed and deployed in ways that are demonstrably safe for children. This includes ensuring that AI-chatbots are not only labelled, but that they do not provide advice or guidance on sensitive topics without appropriate safeguards, validation and clear limitations. AI systems can inadvertently offer misleading or developmentally inappropriate suggestions, particularly in response to children's queries related to mental health, relationships, or body image and should therefore be subject to strict content boundaries and human oversight.

Making it as easy to report illegal and harmful content as it currently is to "like" or "share" content

The Danish Government welcomes the Commission's focus on reporting and namely on how the online platforms should make it easy for minors to report illegal, harmful or other problematic content. The sharing and promotion of illegal or harmful content remains a core problem of especially social media platforms.

A Danish study has found an increase in all the different kinds of unpleasant experiences minors can encounter online in the years between 2021 and 2024. Accordingly, 32 pct. of Danish children have experienced violent photos or videos, they did not want to see. 10 pct. have experienced threats or blackmailing, which is double the number reported in 2021. 9 pct. have seen their private or intimate photos shared against their will, against 3 pct. in 2021.

Despite of an increasing focus on the need to protect minors online and in spite of the fact that the DSA has entered into force in this time period, the changes we see, are not for the better. In Denmark, the experience is that minors seldomly utilise the option of reporting illegal content to the online platforms, as they either are not aware that this option exists or as they find it difficult to report the content in practice. In order to ensure that the reporting mechanisms put in place by the DSA have an actual effect when it comes to protecting minors, we find that the guidelines should recommend that online platforms make it as easy to report content as it currently is to "like" or "share" content.

Further, special consideration should be given to the online platforms' treatment of feedback received from minors. The text should be strengthened to ensure that feedback from minors is not only accommodated, but actively prioritized. Both with a view to enable swift takedown of harmful content spreading through sites populated by minors, but also with a view to learn from minors' perceptions of harmful content. Minors' experiences, needs and perceptions of harm often differ significantly from those of adults and their feedback may reveal distinct risks related to exposure to harmful content. We therefore urge the Commission to recommend that providers of online platforms are required to collect and analyze children's feedback separately from that of adults as a distinct category. The resulting findings should be directly reflected in platform decision-making processes concerning moderation and in adaptations of recommender system and interface design.

Annex: Specific Comments

PROPOSED CHANGES (non-exhaustive, but provided to give an indication);

Ref. (from line)	Current wording	Proposed new text	Justification
231	Before deciding whether to put in place any age assurance method, providers of online platforms accessible to minors should always conduct an assessment to determine whether such a method is appropriate to ensure a high level of privacy, safety and security for minors on their service and whether it is proportionate, or whether such a high level may be achieved already by relying on other less far-reaching measures	Providers of online platforms accessible to minors should implement appropriate age verification measures as a standard protection mechanism – preferably based on the technical specifications and standards used by the EU Age Verification App and the EUDI Wallets. Alternative approaches may be implemented when the provider can demonstrate with clear evidence that such alternatives deliver equivalent or superior protection for minors.	The current wording is problematic because it: 1. Positions age verification as an exceptional measure requiring special justification 2. Characterizes age assurance as potentially disproportionate or "far-reaching" 3. Creates a presumption that alternatives should be preferred The proposed amendment properly recognizes age verification as a fundamental child protection tool rather than a burden requiring special justification. It aligns with our established understanding of comprehensive online risks to minors while ensuring proportionate implementation tailored to each service.
259	Any other circumstances in which the provider of an online platform accessible to minors has identified high risks to minors' privacy, safety or security, including contact risks as well as content risks, that cannot be mitigated by other less intrusive measures	DELETE	We find it problematic that it is the provider of the online platform which solely evaluates and assesses the risk. This enables platforms to prioritize business interests over minors' safety. In case the above line 231 is amended, this part can be deleted.
284	Where the provider of the online platform has identified at least medium risks to minors on their platform as established in its risk review (see Section 5 on Risk Review) and those risks cannot be mitigated by less restrictive measures.	DELETE	Same as above. Additionally, the guidelines appear to accommodate existing technological constraints by requiring less rigorous age assurance measures for platforms with age thresholds below 18, despite these platforms potentially posing significant risks to younger minors. Age

			verification should also be usable for these services.
290	Providers of online platforms accessible to minors that are confronted with those two scenarios may also opt to put in place age verification methods instead. In any event, providers should conduct a proportionality assessment justifying the adoption of age assurance measures prior to putting them in place.	Providers of online platforms accessible to minors that are confronted with those two scenarios are encouraged to put in place age verification methods to complement any age estimation measures. ~~In any event, providers should conduct a proportionality assessment justifying the adoption of age assurance~~ measures prior to putting them in place.	Privacy preserving age verification should always be encouraged where possible. The current wording seems to hint that it is an extraordinary measure not to be used unless necessary. We disagree with this approach (see also counterarguments section above)
	EU age verification solution, including an app, will be an easy-to-use age verification method that can be used to prove that a user is 18 or older (18+).	EU age verification solution, including an app, will be an easy-to-use age verification method that can be used to prove that a user is 18 or older (18+) and in many Member States also other relevant age groups.	Adjusting the wording is necessary to reflect that +18 is not the only age possible to verify – for many MS it should be possible to obtain and issue age attestations of other age groups (+13) or (+15) for example.
1020	The Commission will review these guidelines as soon as this is necessary in view of practical experience gained in the application of that provision and the pace of technological, societal, and regulatory developments in this area.	The Commission will review these guidelines as soon as this is necessary in view of practical experience gained in the application of that provision and the pace of technological, societal, and regulatory developments in this area, and in no later than 5 years.	Timely review of the guidelines will be necessary in order to evaluate their effectiveness, incl. their proportionality. As stated, the area is quickly developing. The general evaluation of the DSA can also lead to updates, which will need to be reflected in the guidelines. This proposal does not preempt the Commission to review the guidelines sooner than 5 years, should they deem it relevant.