ministry of digital affairs

Case no.
2024 - 2955

Document no.
103429

Date
29/10/2024

The Danish government's response to the Commissions call for evidence regarding Article 28 of the Digital Services Act.

Firstly, the Danish Government would like to express its appreciation for the chance to respond to this consultation. Protecting minors online is a huge priority of the government to which strong enforcement and effective implementation of the DSA is pivotal. Accordingly, we agree with the Commission that the heart of the DSA's approach to the protection of minors is article 28(1) and therefore urge the Commission to be ambitious in developing the guidelines as they will be a highly appreciated addition to ensuring effective and smooth enforcement of article 28 in all Member States.

In this regard, we are closely following the Commission's formal proceedings against Meta and TikTok, as these cases concern the protection of minors. It is of particular interest to examine the interaction between the provisions on systemic risk in article 34 and 35 and article 28, which are relevant in the case concerning Meta. We support further work along these lines in the continued enforcement actions under the DSA, as outlined in the mandate of Commissioner-Designate Virkkunen.

In the following, we elaborate our key priorities for the guidelines:

- Following a risk-based approach to the protection of minors
- Making use of default settings to ensure a baseline of safety for minors
- Moving forward on effective and privacy-preserving age verification
- Considering systems for selecting and displaying advertisements

Risk-based approach to the protection of minors

We encourage and fully support the Commission's willingness to take an inclusive approach and allow the guidelines to have a broad scope of application across design, features, functioning and use of platforms that are accessible to minors.

Consideration should be given to creating guidelines that consider the fact that many online platforms have mixed target groups and users. This entails outlining clear and practical definitions of what constitutes inappropriate content for children and young people and how the particular type of content should be categorized based on its harmful nature. As a potential contribution hereto, a national study authorized by the Danish Parliament on the definition of harmful content and functions is currently under development. If the guidelines categorize platforms such as e.g. pornography, gaming, social media etc. and identify the typical risks of these particular types of platforms, it will help the specific industry to identify and mitigate risks.

The protection of minors online presents a multitude of concerns regarding lack of effective age verification, harmful content, harmful commercial practices, excessive collection of minor's user data as well as the effect of online platforms on minors wellbeing etc. Particularly, the exploitation of minors' limited cognitive skills and the commercial or other improper processing and dissemination of their user data gives rise to the need for protection of minors from exposure to content that is harmful and not age-appropriate.

The Danish Government recommends a restrictive approach, where we acknowledge that minors have a right to access the benefits that the services can provide under the parental supervision or with parental consent and to the extent that they are not harmful to them. However, it is important to underline that parental supervision does not alleviate in any way the responsibility of platforms to protect minors from age-inappropriate and harmful content. The guidelines should take this into account as such an approach will enable the engagement of minors and force the industry to focus on the promotion of experiences that are safe and age-appropriate to minors.

Nevertheless, social media and gaming platforms are primarily driven by the companies' financial considerations. This sometimes takes rather extreme forms, where the services through game elements and microtransactions exploit children and young people financially. The Danish Government believes that action should be taken against these forms of practices. Examples of this are loot boxes and in-game currencies.

Hence, the Danish Government supports the Commission's intention to use risk-based standards that apply across the EU. These standards should be enforced consistently across Member States, ensuring that all relevant online platforms adhere to the same level of protection in order for all minors in the EU to enjoy the same protection.

To support the Commission's work to define the best interests of minors in the digital area, we emphasize the need to examine the online experiences of minors and their perspectives, as outlined in the Political Guidelines for the Next European Commission.

Default settings that ensures a baseline of safety for minors

Default settings play a crucial role in protecting minors online by offering a baseline of safety without requiring a proactive effort from the minor. They typically restrict access to age-inappropriate content, shielding children from harmful material.

The guidelines may elaborate on which default settings platforms should put in place. This may include time notifications, financial spending limits, or the basic possibility of activating a consent requirement for financial spending Depending on the individual case, other monitoring and control options with regard to content that can impair the physical, mental or moral development of minors could be considered. Default settings may also include features being turned off for minors and giving parents better tools to monitor and control how minors use different services. Mechanisms such as "geolocation", "seen" and "read" could be turned off as a default setting for minors. It could also be considered whether the "like" function should be made less visible, e.g. not showing to minors how many likes you get. Functions such as "streak", "infinite scroll", "auto play", and algorithmic "feed display" or algorithmic friend recommendations could also be prohibited or minimized towards minors as a default setting.

Default privacy settings may also be useful for limiting the sharing of personal information, helping to prevent unwanted contact. Defaults can disable location tracking and ensure that interactions on platforms are limited, minimizing exposure to online predators or cyberbullying. This also entails ensuring that user profiles of minors cannot be found by search engines, and that contact details and the communication of underage users are not published. The visibility of the profile of minors can be limited to a self-selected group of people and unwanted contact by strangers made impossible. Default settings create a consistent layer of protection, ensuring that even less tech-savvy families benefit from safety measures, reducing the chances of minors being accidentally exposed to risks.

When a service that may contain content only suitable for adults is accessible to both minors and adults, the service should be designed in a way that is considered safe for minors to use (safety-by-design). This means that the service by default must design its algorithms, functions, design, availability, etc. in such a way that all users, including minors, will not be able to access non-age appropriate content/functions and meet the highest level of security as standard. Older users will be able to change this by changing the default settings.

Effective and privacy-preserving age verification

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. It should be as clear as possible that an "age gate" based on the self-declaration of a user cannot be used as an argument that a platform is aware that its users are not minors.

The Danish Government fully supports the need for a harmonized legislative and regulatory framework at EU level to avoid fragmentation within the digital single market. We support that age verification principles and other requirements must be integrated into a mandatory harmonized framework that ensures uniform levels of protection for minors in all EU member states.

To this end, the Danish Government fully supports ongoing efforts and the Commissions intention to make use of the EUDI Wallet as the common and trusted public tool for age verification available for all citizens across EU, not least considering its privacy-preserving potential and the obligation in the EIDAS2 Regulation of VLOPs to facilitate the use of EUDI Wallet.

In the context of the guidelines and given the urgency of the matter, we need to wholeheartedly consider what can be done as we await the full implementation of the EUDI Wallet. To this end, it is very positive that the Commission has announced that it is working on an intermediate "age verification application" to be aligned with the upcoming EUDI Wallet and functional already in 2025. While further details regarding the project are needed, it is evident that such a solution can only become a success if the Commission pursues a coordinated and collaborative approach with timely involvement of relevant stakeholders, including especially Member States. It should also be possible for Member States to develop their own wallet solution and work in line with the age verification application as long as the same technology is used.

We also support the work of the taskforce on age verification established by the Commission to develop practical standards for age verification to ensure a high level of privacy, while underlining the importance of synergies and coordination between different ongoing age verification efforts.

Porn sites, Social media, gaming and gambling platforms are of particular relevance due to their content type and wide range of users. The guidelines should therefore particularly address how these types of platforms should implement age verification and what the minimum requirements are to be in accordance with the DSA.

The guidelines should touch upon how GDPR and the protection of minors regarding data privacy and data handling comes into play regarding age verification and profiling. Data minimization is part of this, meaning that any system must be designed to limit the collection of personal data to what is strictly necessary for the verification, and thus not keep the data when the verification is completed. It should also be clear that the personal data cannot be used for other purposes, including commercial purposes.

Systems for selecting and displaying advertisements

A separate issue is advertisements shown to minors by particularly influencers which pertains to e.g. weight loss drugs and dangerous products and unhealthy foods and drinks. We believe that there should be increased requirements for transparency in influencer marketing and advertising on social media, especially when it comes to the protection of minors.

To ensure that the DSA and UCPD complement each other, the Danish Government recommends that the Commission looks at whether article 5, 6 and 7 in the UCPD should include requirements to present advertisements on online interfaces in a way that corresponds with the requirements in article 26 in the DSA. Thus, all commercial content on online platforms should be marked using a commercial disclosure mechanism provided by the platform. Article 28 does not concern advertising specifically, but we urge the Commission to consider whether the guidelines for article 28 should touch upon standardized advertising for minors.