Feedback on the guidelines on DSA Art. 28 protection of minors - Offlimits

Feedback survey: [Commission seeks feedback on the guidelines on protection of minors online under the Digital Services Act | Shaping Europe's digital future](#)

General Comment
- Completeness
  - There is a lack of precise definitions and minimum standards.
  - There is a lack of parental controls and their perspectives, as well as a consent system for parents/guardians of minors.
  - No mention of VPN— there should be measures in place regarding the use of VPN as well, as currently 25% of the population uses VPN solutions. Easily accessible VPNs make it easy for minors to go around age verification measures.
  - A clear timeline of the enforcement of the guidelines should be included.
  - The lack of the online gaming sector where online abuse of minors is prevalent.
- Challenges
  - The Guideline provides a lot of space and flexibility for online platforms to choose how to comply with the provisions. Therefore, the level and quality of implementation may vary widely, depending on each platform's interpretation and willingness. This raises concerns about the lack of strong enforcement mechanisms and whether such flexibility will lead to meaningful and consistent protection for minors across platforms.
  - While the new Guideline outlines several important measures for online platforms to enhance the protection of minors, how does the Commission intend to ensure consistent and effective compliance across all platforms? Given the broad scope and varied nature of these services, ensuring enforcement may be challenging.
- Suggestions
  - The guidelines should make age verification mandatory for those online spaces, especially where minors are at risk of grooming, gambling, buying products such as alcohol and adult content.
  - The Guideline should use clearer and more precise language, particularly when referencing key terms such as "accuracy," "reliability," "acceptable" and "regular" and "high risk" and "medium risk". Establishing concrete definitions or minimum standards for these concepts would help ensure consistent interpretation and implementation of the guidelines across platforms.

- Collaboration across platforms should be strengthened more throughout the guidelines, to reduce fragmentation in the methods used, making it easier for minors to understand and navigate safety measures.
- The guidelines should be more future-proof (besides the 5th C in the annex), as this will not be revised any time soon.
- The guidelines should include the online gaming sector.

Comments per section
- Risk review
    - The assessment of the risks should not be entirely up to the provider of the service, and the text of the terms and conditions of the service provider should not be decisive.
    - Line 185 – word change: … functionalities, number and type of users and uses (actual and expected) "are" all relevant.
- Age assurance
    - We urge to make age verification **mandatory** on online spaces where minors should not be allowed to access (for example, gambling and pornographic content). Same counts for those online places where adults can groom children, where adults might pose as minors because age verification is lacking. There should be specific guidelines on how to avoid adults from pretending to be minors using age assurance. For example,
        - Line 329— word change: A method that is easy for "minors and adults" to circumvent will not be considered robust enough…
    - **Age verification should be the standard** for any service posing risks to minors, be it high risks or medium risks. Age estimation should be used only in exceptional circumstances, where a service does not pose any risk at all to minors and no personal data are processed.
        - Article 8 of the GDPR states that processing of personal data of a minor under sixteen always requires parental consent: where the child is below the age of 16 years, processing of personal data shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Therefore, in this case, service providers should know whether a user has reached the minimum age of digital consent for processing personal data.
            - The Good practices set forth under line 838 and 1017 should refer to users of 16 and older, or specify that below the age of 16 parental consent is required.
        - Line 297: When grooming is a risk, for example on social media or gaming platforms, age verification should be the standard measure.
    - Line 253-255: In addition to pornographic content, "other 18+ content (e.g. violence)" should be included.

- o Line 259: It should not be up to the provider of the online platform to identify high risks. This should be rephrased to: "Any other circumstances in which the online platform accessible to minors *poses* 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."
- o Line 274: What is the standard of an "equivalent level of verification as the EU age verification application"? How to determine it? Clearer guidance on this should be specified.
- o Line 276: We suggest to make the EU age verification mandatory, on an OS level integrated, for those environments that ask for a strict age. Such as gambling (18), adult websites (18) and as well those places where young people can be groomed, such as social media and online gaming.
- o Line 299 & 314: What is the acceptable margin of error? What is the standard of "accurate"? Clearer guidance on this should be specified.
- o The guidelines should aim at encouraging cross-platform cooperation and establishing an ecosystem approach, as people are always looking for another site or platform that allows them to go around the regulations. An eco-system approach will allow a more comprehensive protection without loopholes, for example that the ID does not have to be checked again for every environment, but that this is done only once.
- Account setting
  - o Line 414-416: "Endless scrolling" should be included as an example of excessive use.
  - o Line 417-421: Any functionalities that repetitively nudge minors to take their agency away should be avoided (for example, Snap constantly asking to "add your contacts" in the opening).
  - o Line 422: In addition to filters, digitally altered content (such as AI generated) should also be included. Concrete examples should also be provided.
  - o Line 482-493: It should not be for the minors to "decide" whether or not to be exposed to persuasive features. The most harmful design-elements should be taken out for minors.
- Online interface design and other tools
  - o The design should not allow adults to register as a minor on the service, as this increases the risk of grooming considerably.
- Recommender system and search feature:
  - o Line 558: Content flagged by trusted flaggers should be removed and not even recommended to anyone at all, especially to children.
- Moderation:
  - o Line 714: Trusted Flaggers should be mentioned as important "relevant stakeholder", as Trusted Flaggers play an important role under the DSA in

flagging and detecting illegal content, and their reports should be prioritised.
- User Support settings
  - Line 807: Insafe network (Helpline) should be mentioned next to the INHOPE network (Hotline) as part of the Safer Internet Centre.
- Monitoring and evaluation
  - Line 947: What is the standard of "regularly monitoring"? There should be a minimum threshold in the Guidelines.

Additional contribution: Information about Offlimits being the first Dutch Trusted Flagger designated under the DSA, and elaborate on Offlimits' role and expertise