

(English version)

**Question for written answer E-001173/26
to the Commission**

Catherine Griset (PFE), André Rougé (PFE), Jean-Paul Garraud (PFE), Pierre Pimpie (PFE), Valérie Deloge (PFE), Julie Rechagneux (PFE)
(20 March 2026)

Subject: Age verification procedures: risks to privacy and data security

As part of measures aiming to restrict minors' access to social media, platforms are required to verify the age of users effectively.

Some low-risk verification methods exist, such as checking how long an account has been active or whether a payment method has been registered.

However, other methods rely on the transfer of sensitive data, such as proof of identity or facial recognition, often through a third-party authenticator. As a result, they pose significant risks to privacy and data security, owing to a mass rise in hacking (now facilitated by artificial intelligence). On top of this, the platforms concerned are obliged to share their information with certain states, including third countries.

1. Will the Commission commit to not forcing platforms to adopt age verification procedures that could be hacked?
2. How can we protect our fellow citizens from multiple national, European and foreign public authorities seeking to use age verification and digital identification to extend their surveillance at the expense of our fundamental rights?
3. Why not introduce measures designed to limit time spent on social media, which would be inherently less intrusive?

Submitted: 20.3.2026

Answer given by Executive Vice-President Virkkunen on behalf of the European Commission
(19 May 2026)

The guidelines on the protection of minors ⁽¹⁾ under the Digital Services Act (DSA) ⁽²⁾ set out guidance for where age assurance technologies should be deployed.

They include minimum specifications to ensure that age assurance measures are accurate, robust, non-intrusive, reliable, and non-discriminatory.

The guidelines are aligned with European Data Protection Board guidance ⁽³⁾, requiring platform providers to only process data that is necessary for age assurance purposes, and to ensure that data processed for this purpose is not stored or used for other purposes.

The Commission developed an age verification solution ⁽⁴⁾ allowing users to prove they are 18+ online. A blueprint is available to Member States for customisation and publication.

Designed to meet the highest privacy standards, it uses 'zero-knowledge proof' technology to securely prove that the user has a valid age credential without revealing the credential or any other information.

The user's identity is only checked once during the issuance of the proof of age. The proof does not contain any identity data, only disclosing that the user is 18+.

The trusted proof provider is not informed about online services for which the proof is used. On 29 April, the Commission adopted a recommendation urging Member States to accelerate the rollout of the age verification app and make it available by the end of 2026 ⁽⁵⁾.

Under the DSA, online platforms accessible to minors are required to provide them a high level of privacy, safety, and security. The aforementioned guidelines outline steps that platforms can take to do so, including to reduce addictive design.

⁽¹⁾ https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C_202505519.

⁽²⁾ <https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng>.

⁽³⁾ https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-12025-age-assurance_en.

⁽⁴⁾ <https://digital-strategy.ec.europa.eu/en/factpages/blueprint-age-verification-solution-help-protect-minors-online>.

⁽⁵⁾ <https://digital-strategy.ec.europa.eu/en/news/commission-urges-member-states-rollout-eu-age-verification-app>

The Commission recently adopted preliminary findings against TikTok ⁽⁶⁾ where the Commission informed the provider that they must disable features that can contribute to excessive use.

⁽⁶⁾ https://ec.europa.eu/commission/presscorner/detail/en/ip_26_312.