

(English version)

**Question for written answer E-001010/25
to the Commission
Miriam Lexmann (PPE)
(7 March 2025)**

Subject: Strengthening age verification through app stores and operating system providers

The Digital Services Act (DSA) sets out clear risk-based obligations to protect minors online. However, there is currently no clarity on when and where age verification (AV) should be used. App stores and operating systems are uniquely positioned to provide a unified, privacy-preserving, secure and efficient solution by verifying users' ages at device or app store level and sharing an assured age signal with third-party apps. Such a system would prevent repetitive age checks, restrict underage users from accessing inappropriate content and better align with the requirements of the DSA and the Digital Markets Act.

In this context:

1. Has the Commission thought about supporting app store or device level AV solutions, such as those that exist in other jurisdictions such as Singapore and the US states of South Dakota and Utah?
2. Will the Commission acknowledge in the upcoming guidelines on Article 28 of the DSA that app stores, as gateways to multiple services, pose a higher level of risk compared to the potential risks posed by individual apps, and that AV at this level might be necessary to mitigate that risk?
3. Will the Commission acknowledge in the upcoming guidelines on Article 28 of the DSA that app stores, as very large online platforms and gatekeepers, have a special responsibility in the value chain to protect minors online?

Submitted: 7.3.2025

**Answer given by Executive Vice-President Virkkunen on behalf of the European Commission
(5 May 2025)**

The regulation on the establishment of the European Digital Identity (EUDI) Framework ⁽¹⁾ mandates Member States to offer digital identity wallets. It provides the possibility for effective age verification (AV) within the EU.

To bridge the gap until the EUDI wallets become available, the Commission is developing a privacy preserving, data minimising, harmonised AV solution.

Under Article 28(1) of the Digital Services Act (DSA) ⁽²⁾, all providers of online platforms accessible to minors must ensure a high level of privacy, safety and security to minors on their services.

Those providers of online platforms accessible to minors, including app stores (i.e. Google Play), must implement appropriate and proportionate measures to fulfil such obligations.

Independently from app stores' obligations, some app developers distributing their apps on app stores (i.e. TikTok) also fall under the scope of Article 28(1) of the DSA. To comply with that provision, providers of online platforms accessible to minors may have to implement AV, based on their risk profile ⁽³⁾.

Providers of app stores designated as very large online platforms are required, under Articles 34 and 35 of the DSA, to identify, analyse and assess the systemic risks stemming from the design, functioning or use made of their services, considering *inter alia* any actual or foreseeable negative effect for the respect of the rights of the child enshrined in Article 24 of the Charter of Fundamental Rights of the EU ⁽⁴⁾, and put in place effective mitigation measures to address such risks.

⁽¹⁾ Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework (OJ L, 2024/1183, 30.4.2024).

⁽²⁾ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (OJ L 277, 27.10.2022).

⁽³⁾ The Commission will set out in Guidelines in which scenarios it would expect online platforms to implement age verification or age assurance in order to ensure a high level of privacy, safety and security.

⁽⁴⁾ Charter of Fundamental Rights of the EU (OJ C 326, 26.10.2012).