

**Question for written answer E-002262/2024
to the Commission**
Rule 144
Elena Kountoura (The Left)

Subject: Incomplete rules on the protection of privacy and personal data in the Commission's implementing acts for the European digital identity wallet

Serious concerns have been raised¹ concerning the gaps that exist in the Commission's implementing acts, which establish the technical features of the European digital identity wallet (eIDAS)², regarding the protection of privacy and the personal data of EU citizens.

Despite the additional reassurances given by the European Parliament and the Council in the new eIDAS regulation, the current implementing acts do not fully reflect these requirements, leaving major gaps in user protection. Specifically:

- A clear mechanism for limiting the data that relying parties are allowed to ask for is lacking, exposing users to requests to hand over too much personal data and to excessive personal data collection;
- Complaints and requests to have data deleted are not handled in the same way across EU countries, which limits the rights afforded under the GDPR³;
- The regulatory provisions do not guarantee unlinkability⁴ and unobservability⁵, making surveillance of user transactions possible, in violation of the eIDAS regulation.

In view of this:

1. How does the Commission plan to ensure full compliance with the requirements of the GDPR and the eIDAS regulation with regard to the protection of privacy and guaranteed unlinkability and unobservability?
2. What steps will it take to ensure the interoperability and cross-border harmonisation of processes for lodging complaints and requesting data deletion, so as to harmonise the rights of users across the EU?
3. How does it plan to ensure the deterrence of requests for too much personal data and the excessive collection of user data?

Submitted: 25.10.2024

¹ <https://epicenter.works/en/content/eidas-implementing-acts-european-digital-identity-wallets>

² The Commission is obliged to issue a series of implementing acts to further elaborate on certain articles within the regulation.

³ The GDPR lays down data protection principles, such as data minimisation and purpose limitation, as well as obligations, such as data protection by design and by default. The eIDAS application must comply with these principles and obligations.

⁴ Under eIDAS, the technical framework must not allow providers of electronic attestations of attributes or any other party to obtain data for the purpose of tracking, linking or correlating user transactions and behaviour.

⁵ The eIDAS regulation stipulates that European wallet providers must guarantee unobservability by not collecting data and by not having knowledge of user transactions. However, the implementing acts do not explain how this protection will be guaranteed.