

Spanish Data Protection Authority

AEPD, Agencia Española de Protección de Datos

Calle Jorge Juan, 6. 28001 Madrid, Spain

<https://www.aepd.es/>

División de Innovación Tecnológica

dit@aepd.es

Response to ARF Discussion topics:

Topic L+M “Requesting erasure of personal data at a wallet-relying party and lodging a complaint with the competent data protection supervisory authority”

Any analysis on these topics must begin by identifying the personal data processing activities that occur and assigning the controller/processor roles for each. Otherwise, meaningful discussion about the different obligations, the data subject's exercise of rights, etc., is impossible.

At this point in the discussion, we would like to make the following observations concerning the available information:

- The discussion paper suggests that a Wallet Unit should provide an interface to report suspicious requests from a Relying Party to the DPA of the Member State that provided the Wallet Unit. This approach potentially restricts the right of users under Article 77 of the GDPR to interact with a DPA in the Member State of their habitual residence, place of work, or place of the alleged infringement.
- We find it particularly worrying that reporting suspicious requests may pose an identification threat in use cases where the user requires anonymity. What mechanisms exist to present these reports anonymously from the Wallet Unit? This could be explicated in the HLR RPT_DPA_04.
- In this regard, it is probably necessary to clarify whether the HLRs under RPT_DPA refer to “lodge a complaint” within the meaning of the GDPR (some DPAs do not allow this to be done anonymously), or to report suspicious behavior, which can be done as a concern or tip-off. This can be always done anonymously.
- The discussion paper states that “*According to Article 5a (a) of Regulation (EU) No 910/2014 a wallet solution shall support common protocols and interfaces for (ix) requesting a relying party to erase the personal data stored at a wallet-relying party pursuant to Article 17 of Regulation (EU) 2016/679*”. But this is not correct, since, as specified in the HLR DATA_DLT_01 “*A Wallet Provider SHALL ensure that its Wallet Units support the technical specifications mentioned in DATA_DLT_02, allowing a User to request from a Relying Party the erasure of their attributes that were presented by that Wallet Unit to that Relying Party*”. Therefore, we are not considering the erasure of any personal data but the erasure of attributes that were presented by the Wallet Unit exclusively.

- The discussion paper addresses the technical specifications for a Wallet Unit interface to send attribute deletion requests to Relying Parties. However, we are concerned about the lack of EU-wide harmonization for deletion requests, potentially leading to GDPR data subject rights being respected only in the Member State where the Wallet was issued. We would like to know how the right to erasure will be enforced in cross-border scenarios.
- While the need to authenticate data erasure requests is acknowledged, the discussion paper does not provide details on the specific mechanisms. If these mechanisms are not robust and privacy-preserving, they could lead to unauthorized data erasure or create new avenues for profiling or tracking users.
- In general, the lack of specific technical interfaces for cross-border complaints and deletion requests could be interpreted as a failure to adequately integrate data protection safeguards into the design of the EUDI Wallet ecosystem (Article 25 of the GDPR, data protection by design and by default).