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 N "Export and data portability"

Any analysis on these topics must begin by identifying the personal data processing activities 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:

- Concerns exist regarding the scope of data to be logged by the Wallet Unit, which includes the type of data requested and presented in transactions, documents or data signed and information about the issuance or re-issuance transactions. While logging transaction data serves purposes like providing users with a transaction history, the extent of this logging must be proportionate and limited to what is necessary for the specified purposes (e.g., transparency for the user, potential dispute resolution, etc.). What legitimate purposes justify, in each case, all the logs that are established to be collected and stored? HLRs such as DASH_03, DASH_04 and DASH_05 should be examined under this data minimisation and purpose limitation lens.
- Furthermore, these requirements only establish a minimum data set to be logged ("*at least*"). This opens the door to even more detailed logs.
- Wallet providers are responsible for ensuring the confidentiality, integrity, and authenticity of the logged information. Given the sensitivity of some logs, any vulnerabilities that allow for tampering with the data or unauthorised access may violate users' fundamental rights. Therefore, we advise establishing specific requirements concerning log/dashboard protection. The HLR DASH_07 is too vague.
- The data exported for portability should be used solely to enable the user to migrate to a different wallet solution or to access their data. Using the Migration Object for any other purposes by the new wallet provider or any other entity without a lawful basis and informing the user would constitute an infringement (purpose limitation, Article 5(1)(b) of the GPDR).
- The discussion paper emphasises the need for secure export and portability of personal data. This includes ensuring the data's confidentiality, integrity, and authenticity during the export and import processes. Weak or inadequate security

measures during these processes could lead to unauthorised access, data breaches, or manipulation of the exported data. Therefore, we advise establishing specific requirements concerning the protection of the Migration Object in different locations and of the import/export processes. The HLR Mig_05 is too vague.

- Users need to be provided with clear and comprehensive information about what data will be exported, the process involved in data portability, any limitations (like the need for re-issuance), and the security measures in place. Lack of transparency or providing misleading information would infringe the GDPR's transparency principle and requirements.