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 T "Support and Maintenance by the Wallet Provider"

Support and maintenance of the EUDI Wallet may involve crucial data processing activities that must be designed with strict adherence to GDPR principles and requirements. Any functions related to maintenance, technical support, incident response, or recovery by Wallet Providers (WPs) must be carefully assessed to prevent infringements of fundamental user rights, particularly concerning tracking and surveillance.

We would like to make the following observations concerning the data protection implications of Wallet Provider support and maintenance activities:

- Strict adherence to data protection principles: All data processing carried out by the Wallet Provider for support and maintenance must be limited to what is strictly necessary for the provision of the Wallet services (data minimisation and purpose limitation). For example, any processing of personal data in the logs must be collected for specified, explicit, and legitimate purposes. The primary purpose is to provide users with a transparent history of their activities and enable them to exercise their rights. Processing these logs for undisclosed purposes beyond what users reasonably expect would violate the principles of lawfulness, fairness, and transparency. What specific High Level Requirements support this adherence? We recommend providing explicit guidance on what personal data the Wallet Provider is permitted to collect from Wallet Instances for each specific mandatory support and maintenance purposes: installation of a new version of the Wallet Solution, WUAs update, Wallet Unit revocation (in case its security is compromised, for example), regular updates of the Wallet Instance application, etc. Additionally, we recommend including a HLR mandating Wallet Providers to list, in advance, any other support and maintenance activity *necessary for the provision of Wallet services*. The proposed list would serve to formally delineate these specific, necessary processing activities, ensuring they have a legal basis, a specific purpose, etc.
- Unobservability during support activities: Support and maintenance operations pose a direct threat to the principle of unobservability, which mandates that WPs should not have insight into the details of the users' transactions. While Wallet Providers are required to ensure users can easily request technical support and report technical problems or other incidents, the mechanisms established for reporting and diagnosis

must uphold the requirement that the technical framework does not allow Wallet Providers to link, correlate, or track transactions or user behaviour. If access to transaction data is genuinely required for diagnostic purposes (e.g., investigating a reported technical issue), this should only be granted in specific cases, on an instance-by-instance basis. Again, we recommend providing explicit guidance on what personal data the Wallet Provider is permitted to collect from Wallet Instances for each specific mandatory support and maintenance purpose, such as providing technical support, investigating a technical problem, or incident.

- Data separation as a foundation for compliance: The eIDAS 2.0 regulation requires that personal data related to the provision of the European Digital Identity Wallet be kept logically separate from any other data held by the provider. This includes data gathered during support or maintenance activities. This measure is essential to prevent the Wallet Provider from combining personal data from Wallet services with personal data derived from any other services they offer, thereby preventing misuse.
- Transparency and user control over maintenance: The user must maintain full control over maintenance activities, which must be transparent. The user must be kept informed and involved as a data subject in processes such as revocation or re-issuance and must be allowed to exercise all their data protection rights about these processes, even if explicit user actions are not required. Furthermore, users must be provided with clear and comprehensive information about security measures in place for processes such as data portability (export/import), as a lack of transparency would infringe the GDPR's transparency principle.
- Accountability for data integrity and confidentiality: Maintenance activities, such as implementing recovery processes or facilitating migration, rely on secure handling of the Migration Object. Any vulnerabilities that allow tampering or unauthorized access may violate users' fundamental rights. Therefore, specific requirements concerning the protection of the Migration Object during export and import processes, for example, must be established. The ARF should require WPs to establish procedures for data breaches and conduct regular audits to test security measures (e.g., encryption and access controls).