Cyber Security for Europe

Policy Recommendation

Allocating controllership in the European Digital Identity Wallet

Context and Findings

The **eIDAS 2 proposal** enables the transition towards **new models for identity management (IdM)**, placing the user at the centre of the ecosystem and limiting the role of identity providers (providers of electronic attestations of attributes/ issuing authorities), to the provision of identity credentials (electronic attestations of attributes). In this context, **the European Digital Identity Wallet (EUDIW) emerges as a key piece to empower users in the control of their personal data**, enabling identification and authentication processes through the sharing of credentials with external parties.

The eIDAS 2 proposed ecosystem **displaces the responsibility of identity providers in the authentication process to the wallet**. However, **the wallet**, as a technology that should be managed exclusively under user control, **challenges the General Data Protection Regulation's (GDPR) traditional role for data controllers** as there is no entity, but the user, who should have actual access to the data.

There already exist multi-purpose digital wallets that enable the management of credentials containing users' personal data (e.g., Apple Wallet or Google Wallet). Nevertheless, **the scope of the eIDAS 2 proposal makes necessary legal certainty concerning the allocation of controllership and liability** for the personal data that will be stored in and managed via the European Digital Identity Wallet.

The Problem

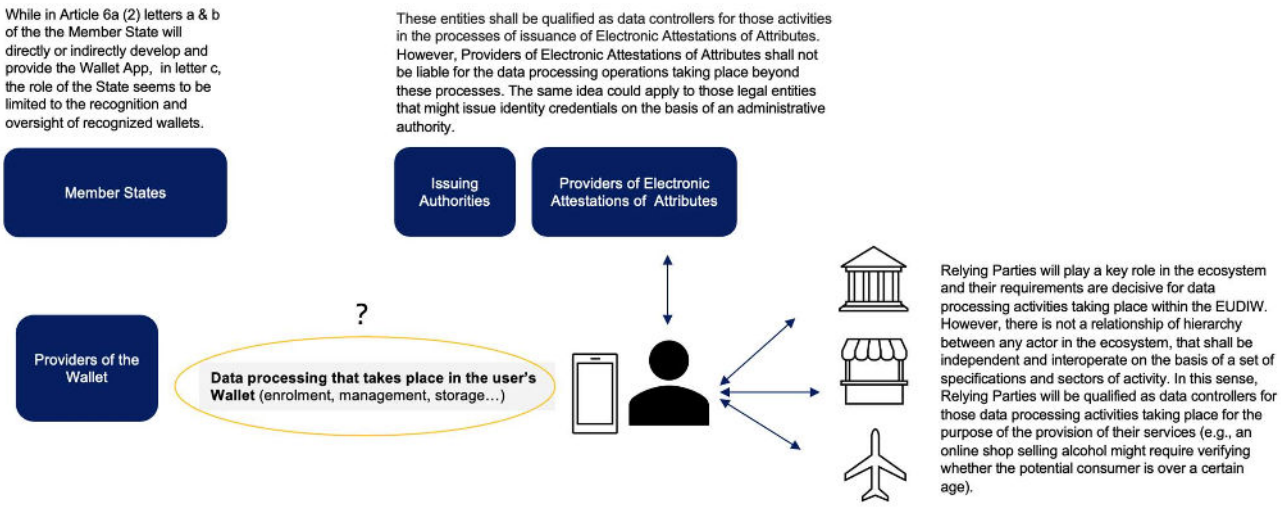
Ascertaining controllership over certain data processing activities is crucial to allocating GDPR obligations and responsibilities. Nevertheless, the EUDIW ecosystem is complex and encompasses different entities, holding various roles and who perform a set of data processing activities with separate purposes, but that are necessary or contribute to the overall functioning of the ecosystem. In particular, the data processing taking place in and via the EUDIW represents a challenge to traditional legal notions of a data controller and data processor according to the GDPR (Articles 4. (7)(8)).

The Scene

Article 6a, section 1, of the eIDAS 2 proposal establishes that “each Member State shall issue a European Digital Identity Wallet”. However, section 2 of this Article envisages three different possibilities for the issuance of the EUDIW. More specifically, section 2(c) envisages the possibility of issuance by private entities and recognised by a Member State. In such a scenario, it will be crucial to determine to what extent implementing acts decide/rule the data processing conditions (regarding the issuance of the wallet app and the requirements in the wallet App itself); and what is the role of Member States is in providing such recognition.

The Implications

The allocation of controllership under the GDPR is essential to determining the obligations and responsibilities of the party that must and can successfully protect a user’s personal data. These obligations should be clearly envisaged in the EUDIW ecosystem; in particular, account should be taken of the possibility of the provision by private entities. Otherwise, the security of a user’s personal data could be left under their exclusive responsibility and in the event of errors, misfunctioning, etc, liability might be complicated to enforce.



Policy Recommendations

The quick developments in the technological landscape require regulations to adapt faster than ever. The **lack of legal studies and adaptation of traditional regulations can be a brake to technology advances** due to the legal uncertainty and the risk for potential stakeholders to deploy a technology. On the other hand, the implementation of technologies without the adequate legal guarantees can result in a situation where there is an absence of legal rights. On this basis, the following recommendations are proposed:

1) **The European Data Protection Supervisor should issue an Opinion clarifying the application of the data controller role to the scenarios described for the issuance of the EUDIW in Article 6a section 2 of the eIDAS 2 proposal.**

   The EUDIW ecosystem is complex, and despite according to Article 6a section 1, issuers of the EUDIW will be Member States, Article 6a section 2 envisages the possibility of the provision of wallet apps by private entities. In principle, insofar as personal data needs to be processed for the provision of the wallet app, these private entities would hold a role under the GDPR. Nevertheless, more challenging would be the circumstance where the wallet provider does not need to process any personal data (the desirable scenario), but still develops software that enables certain data processing activities. Under these circumstances, the allocation of the data controller role might be complicated.

   It should be considered that wallet providers, as the entities developing the wallet app, are concerned with the final purpose of the wallet, and although the user will hold a certain control (e.g., with which parties they share their data), this management will ultimately rely on the application created by the wallet provider. More specifically, the developers of the wallet app pre-define in technical terms how data is collected and for what potential purposes and they hold “interpretative control”; that is to say, they determine how to transform data into actionable decisions.

   It could still be challenging the fact that these entities might not physically process any personal data. However, it should be noted that the European Court of Justice has ruled in several cases that it is irrelevant whether a concerned party has actual access to the data when it comes to ascertaining its controllership (Case Fashion ID C-40/17, Case Jehovan todistajat C-25/17).

   In conclusion, this scenario might represent a less common approach to the concept of data controller, in particular, considering existing IdM ecosystems, where the identity provider has responsibility when personal data is being processed for identification and authentication processes. In the scenario of the wallet, despite wallet providers ideally not having access to personal data, they are still concerned with the final purpose of the wallet and therefore the data processing that takes place in and via the wallet.

2) **Support and provision of funding to conduct research on the impact of innovative technologies in EU regulatory frameworks.**

   The scenario presented above is not unique and technologies are challenging the way traditional legal concepts are understood. It would be worth investigating more in depth the application of traditional GDPR administrative roles (data controller / processor) to the scenarios raised by new technologies, like the EUDIW, but also others such as artificial intelligence or distributed ledger technologies. Such studies would be crucial to understanding if traditional legal concepts remain applicable to new technological developments and might suggest rethinking these concepts to cover upcoming advances.

References

1 D6.3 Final Pilot deployment and evaluation of User Experience and GDPR Compliance. **OLYMPUS Project** *(Oblivious identitY Management for Private and User-Friendly Services)* [Project Deliverable] pp.76-91. https://olympus-project.eu/wp-content/uploads/2021/10/Olympus_pu_d6_3_v1_2.pdf

2 OLYMPUS contributions and recommendations for improving cross-border identification in the European Union. **OLYMPUS Project** *(Oblivious identitY Management for Private and User-Friendly Services)* [Policy Brief]. https://olympus-project.eu/wp-content/uploads/2021/11/Olympus_pu_policy-brief_v1_0.pdf

Contact

This brief was produced by members of the CyberSec4Europe consortium.
Contact person: Professor Antonio Skarmeta skarmeta@um.es / Researcher Cristina Timón mariacristina.timon@um.es

CyberSec4Europe is funded by the European Union under the H2020 Programme Grant Agreement No. 830929. These results reflect only the authors' view and the Commission is not responsible for any use that may be made of the information it contains.