Formal comments of the EDPS on the Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity

1. Introduction and background

- On 3 June 2021, the EDPS was consulted according to Article 42(1) of Regulation 2018/1725[1] on the Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity.[2]
- According to the Explanatory Memorandum, the draft Proposal would address shortcomings of the current Regulation[3] such as the following:
  - limited coverage of eID schemes notified under the current Regulation,
  - limited offers of eIDAS authentication for cross-border users of public services,
  - limitation to public services, albeit a market demand exists in the private sector,
  - no coverage of electronic attributes, such as medical certificates or professional qualifications, making difficult pan-European legal recognition of such credentials in electronic form.
- With the revised European Digital Identity framework, it is intended to give citizens and residents full confidence that it will offer the means of control who has access to their digital twin and to which data exactly.
- A high level of security shall be awarded to all aspects of digital identity provisioning, including the issuing of a European Digital Identity Wallet, and the infrastructure for the collection, storage and disclosure of digital identity data.
- The Proposal expands the current eIDAS list of trust services with three new qualified trust services, namely the provision of electronic archiving services, electronic ledgers and the management of remote electronic signature and seal creation devices.
- The proposed eIDAS Regulation is still comprised of two most important parts, Chapter II (so far titled Electronic Identification) and Chapter III (Trust Services). However, Chapter II is now be divided in three Sections and also Chapter III gains three Sections,

[1] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ, 21.11.2018, L.295, p.39 (Regulation 2018/1725).

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281.

[3] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ, 28.8.2014, p. 73.

amounting to 11 Sections altogether. Chapters IV to VI are not relevant from a data protections perspective.

- The envisaged technical implementation will ultimately determine whether additional data protection safeguards should have been integrated in the Regulation or whether its design will be in accordance with the GDPR[4] at all. However, as was the case with Regulation (EU) No 910/2014, the technical architecture cannot be fully assessed until the up to 28 Commission Implementing Acts are known that are planned to lay down technical specifications and reference standards. Those Acts are also likely to fall within the scope of Article 42(1) of Regulation 2018/1725, and are likely to be subject to consultation of the EDPS in the future. Therefore, the present formal comments do not preclude any future additional comments by the EDPS, in particular if further issues are identified or new information becomes available, for example as a result of the adoption of related implementing or delegated acts.
- The present formal comments of the EDPS are issued in response to the legislative consultation by the European Commission of 3 June 2021, pursuant to Article 42(1) of Regulation 2018/17257. In this regard, the EDPS welcomes the reference to this consultation in Recital 37 of the Proposal. They are without prejudice to any future action that may be taken by the EDPS in the exercise of his powers pursuant to Article 58 of Regulation (EU) 2018/1725.

2. Comments

- The EDPS welcomes the general concept of the Proposal which requires the European Digital Identity framework to be fully in line with Regulation (EU) 2016/679. Whether the specific safeguards are sufficient depends mainly on the technology to be used in implementing the proposal. In this respect, the EDPS welcomes that the Proposal reaffirms in its Recitals the full applicability of the GDPR, also for electronic ledgers and qualified electronic ledgers.[5] This approach is fully in line with Article 25 of the GDPR which requires the choice of technology be made according to the data protection requirements, and not the other way around.
- From the explanatory memorandum, especially on page 10 and 11, it can be derived that electronic ledgers as a trust service will not be a necessary element of the the European Digital Identity Wallet, but will be limited to specific use cases. The EDPS appreciates this clarification. The EDPS appreciates that the explanatory memorandum confirms that Service Providers will need to comply with the GDPR also in use cases for electronic ledgers, and that nothing in the Proposal allows for a deviation from GDPR provisions.
- Blockchain technology is one of those implementing electronic ledgers. Blockchain raises several compliance issues with the GDPR, such as data transfers outside the EU, the impossibility to delete or correct entries in a Blockchain etc. Therefore, the use of

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ, 4.5.2016, p. 1.
[5] Recital 35.

Blockchain technology may not be appropriate for all possible use cases and may require additional safeguards. It should be noted that the European Data Protection Board has included upcoming "Guidelines on Blockchain" in its Work Programme 2021/2022.[6] The EDPS recommends that those guidelines, once available, be taken into account when considering blockchain based ledgers in the context of this Proposal.

- The EDPS welcomes that the European Digital Identity Wallet will give the user better and transparent control on what data to share with whom for what purposes. The technical solution envisaged would be able to solve problems of excessive data processing, as it would allow the data subject to actually reveal only those data that are necessary for a specific purpose. That means, if the purpose is age verification, the user could choose to submit his birth date but withhold disclosing other personal information not relevant to the purpose. If the purpose is identification, for example in the banking or telecommunications sector, as required by law, the user could reveal only those pieces of identity data mandated by law (without biometric identifiers, for example, if their processing is not explicitly required).
- The EDPS further welcomes the explicit prohibition in the new Article 6a(7) for the issuer of the European Digital Identity Wallet to collect information about the use of the Wallet which are not necessary for the provision of the Wallet services. This and the prohibition to combine person identification data for the Wallet with other data from any other service as well as the obligation to physically and logically separate the personal data for the provision of the Wallet services from any other data held will increase the trust in the security and confidentiality of this technical solution.
- In this context the EDPS also welcomes that Article 6c(2) would establish a certification pursuant to Regulation (EU) 2016/679 for certain requirements to European Digital Identification Wallets, including the prevention that trust service providers of qualified attestations of attributes could receive any information about the use of these attributes. The EDPS understands that also this certification is mandatory and will have no exculpatory effects.
- Article 17 contains the tasks of the supervisory body and foresees cooperation with other supervisory authorities, such as those under Regulation (EU) 2016/679. According to this provision, data protection supervisory authorities will be notified "without undue delay about the results of audits of qualified trust service providers, where personal data protection rules have been breached and about security breaches which constitute personal data breaches". The EDPS notes that the wording that seems to require the completion of an investigation, goes back to Article 17 of Regulation (EU) No 910/2014 and constitutes already an improvement over that current version insofar as a personal data breach in the sense of Article 33 of the GDPR would now also trigger the duty to inform. However, the EDPS draws attention of the co-legislator to the fact that the previous wording corresponded to a different role of data protection authorities, whereas Article 33 of the GDPR requires Controllers to notify qualifying data breaches without undue delay, not later than 72 hours after having become aware of them, offering

[6] https://edpb.europa.eu/system/files/2021-03/edpb_workprogramme_2021-2022_en.pdf

supervisory authorities an active role during the investigations of a breach and in the choice of further measures. For this reason, it seems appropriate to align the wording of Article 17(4)(f) to point (c) of the same paragraph, where the national competent authorities pursuant to the NIS2 Directive would be informed of a (suspected) security breach regardless of whether the results of an audit have found a breach. The data protection supervisory authorities should be informed whenever the supervisory body receives information of a possible personal data breach.

- For the same reason, Article 20(2) last sentence should also be aligned with the GDPR and mandate immediate notification, regardless of whether the audit has been finished or is still ongoing.
- The draft proposal introduces a unique and persistent identifier to be used by Member States to facilitate identity matching and ensure the unique identification for each user. This identifier would then *inter alia* be used when adding electronic attestations of attributes to a Wallet.
- The EDPS does appreciate the effort in Article 11a to enhance trust and integrity by reducing the risk of abuse or ambiguity errors. It should, however, be noted that this unique and persistent identifier constitutes another, additional category of data stored solely for the purpose of facilitating the usage of the Wallet. This interference with the rights and liberties of the data subject is not necessarily trivial; in some Member States, unique identifiers have been considered unconstitutional in the past due to a violation of human dignity. Therefore, the EDPS recommends exploring alternative means to enhance the security of matching.
- The EDPS notices that Article 45f further regulates the use of personal data by Providers of qualified or non-qualified electronic attestation of attributes services. They shall not combine personal data relating to the provision of these services with personal data from any other services they offer, and shall keep the data logically separate, in the case of personal data relating to the provision of qualified electronic attestation of attributes services even physically separate, from other data held. It is the EDPS's opinion that these prohibitions cannot be circumvented by means of contractual clauses or consent. The EDPS welcomes these prohibitions as a measure to prevent misuse of data and to increase trust in the system. For Providers of qualified electronic attestation of attributes' services, Article 45f(4) even foresees that such services shall be provided under a separate legal entity, which, in combination with the prohibitions mentioned above, should be an effective mechanism to prevent conflicts of interest and unwarranted sharing of personal data.

Brussels, 28 July 2021

Wojciech Rafał WIEWIÓROWSKI
(e-signed)