EDPS Formal comments on the draft Commission Implementing Regulation (EU) laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council, as regards the integrity and core functionalities of European Digital Identity Wallets

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) No 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of individuals 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 ('EUDPR')[1], and in particular Article 42(1) thereof,

HAS ADOPTED THE FOLLOWING FORMAL COMMENTS:

1. Introduction and background

1. On 13 August 2024, the European Commission consulted the EDPS on the draft Commission Implementing Regulation (EU) laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council, as regards the integrity and core functionalities of European Digital Identity Wallets ('the draft Implementing Regulation').
2. The draft Implementing Regulation is accompanied by annexes[2].
3. The objective of the draft Implementing Regulation is to lay down the rules for the integrity and core functionalities of the European Digital Identity Wallets[3].
4. The draft Implementing Regulation is adopted pursuant to Article 5a(23) of Regulation (EU) No 910/2014[4], as amended by Regulation (EU) 2024/1183 amending

[1] OJ L 295, 21.11.2018, p. 39.
[2] The draft Implementing Regulation is accompanied by four annexes specifying the list of standards referred to in Article 8, the list of common embedded disclosure policies referred to in Article 10, the signature and seal formats to be supported by signature creation applications referred to in Article 12 and the technical specifications for pseudonym generation referred to in Article 14, respectively.
[3] Article 1 of the draft Implementing Regulation.
[4] 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 L 257, 28.8.2014, p. 73–114.

EUROPEAN DATA PROTECTION SUPERVISOR
Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30 - B-1000 Brussels
E-mail: edps@edps.europa.eu
Website: edps.europa.eu
Tel.: 32 2-283 19 00 - Fax: 32 2-283 19 50

Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework ('the EDIW Regulation')[5].

5. The EDPS previously issued formal comments on the proposal for the EDIW Regulation[6]. As stated in the EDPS formal comments[7], the envisaged technical implementation will ultimately determine whether all necessary data protection safeguards have been integrated in the EDIW Regulation or not. Indeed, the EDPS highlights that the technical architecture of the European Digital Identity Wallet cannot be fully assessed until all the relevant implementing acts aiming at laying down technical specifications and reference standards are finalised.

6. The EDPS further highlights that different aspects covered by the implementing regulations interact with and influence each other. For instance, aspects related to the core functionalities are related to the aspects concerning the interfaces of the European Digital Identity Wallet. The EDPS is concerned that the complexity of the overall architecture, combined with a multiplicity of implementing acts, make it impossible to fully assess the impact at this stage.

7. These formal comments therefore do not preclude any additional comments by the EDPS in the future, in particular if further issues are identified or new information becomes available, for example as a result of the adoption of other related implementing or delegated acts[8].

8. The present formal comments of the EDPS are issued in response to a consultation by the European Commission pursuant to Article 42(1) of EUDPR.

9. Furthermore, these formal comments 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 the EUDPR and are limited to the provisions of the draft Implementing Regulation that are relevant from a data protection perspective.

[5] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework, OJ L, 2024/1183, 30.4.2024.
[6] EDPS Formal comments 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, issued on 28 July 2021.
[7] EDPS Formal comments 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, page 2.
[8] In case of other Implementing or delegated acts with an impact on the protection of individuals' rights and freedoms with regard to the processing of personal data, the EDPS would like to remind that he needs to be consulted on those acts as well. The same applies in case of future amendments that would introduce new or modify existing provisions that directly or indirectly concern the processing of personal data.

2. Comments

2.1. General comments

10. Recital (1) of the draft implementing regulation recalls that the European Digital Identity Wallets ('wallets') aim at facilitating access to services across Member States, for natural and legal persons, while ensuring the protection of personal data and privacy. For the sake of completeness, the EDPS recommends adding a recital explicitly recalling the applicability of the EU data protection legal framework when processing personal data within the scope of the draft Implementing Regulation. In particular the EDPS recommends making explicit reference to Regulation (EU) 2016/679 ('the GDPR')[9] and Directive 2002/58/EC ('ePrivacy Directive)[10].

11. The EDPS notes the absence of a reference to this consultation in a recital of the draft Implementing Regulation. Therefore, the EDPS recommends inserting such a reference in a recital of the draft Implementing Regulation.

2.1.1. The EDIW Regulation and data protection by design and by default

12. The EDPS welcomes that the EDIW Regulation contains provisions[11] enabling the implementation of the wallet in accordance with the principle of data protection by design and by default[12]. The draft Implementing Regulation, in turn, should also foster the implementation of this principle, taking into account in particular the state of the art of technology.

13. In the following paragraphs, the EDPS recalls provisions of the EDIW Regulation that are important under a privacy and data protection viewpoint, having regard in particular to the principle of data protection by design and by default.

14. Article 5 of the EDIW Regulation provides that "*[w]ithout prejudice to specific rules of Union or national law requiring users to identify themselves or to the legal effect given to pseudonyms under national law, the use of pseudonyms that are chosen by the user shall not be prohibited*"[13]. Article 5a(4)(b) of the EDIW Regulation further specifies that wallets must enable the users to generate pseudonyms and store them encrypted and locally within the wallet, in a manner that is user-friendly, transparent, and traceable

[9] 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 L 119, 4.5.2016, p. 1–88.

[10] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37–47.

[11] Notably, under Article 5; Article 5a(4), letter (a); Article 5a(14); Article 5a(16), letter (a) and (b) of the EDIW Regulation.

[12] Article 25 of Regulation (EU) 2016/679 ('the GDPR').

[13] Article 5b(9) of the EDIW Regulation further provides that relying parties shall not refuse the use of pseudonyms, where the identification of the user is not required by Union or national law.

by the user. This means that users should be able to use the wallet in such a way that a relying party can, when this is necessary, have visibility on multiple transactions carried out by a specific user without having access to the legal identity of the user.

15. Article 5a(4)(a) of the EDIW Regulation provides that the wallet must ensure that selective disclosure of data to relying parties is possible.

16. Article 5a(4) and (5) of the EDIW Regulation establish in particular the requirements for the security and integrity of the wallet. The latter needs to be uniquely and securely linked to a user, whose personal identification data and attributes must not be at risk of being transferred to a wallet belonging to another user.

17. The EDIW Regulation provides in Article 5a(14) that the users shall have full control of the use and of the data in their wallet.

18. Article 5a(14) of the EDIW Regulation provides that the provider of the wallet must neither collect information about the use of the wallet which is not necessary for the provision of wallet services, nor combine person identification data or any other personal data stored or relating to the use of the wallet with personal data from any other services offered by that provider or from third-party services which are not necessary for the provision of wallet services, unless the user has expressly requested otherwise.

19. Article 5a(16)(a) of the EDIW Regulation provides that the technical framework of the European Digital Identity Wallet must not allow "*providers of electronic attestations of attributes or any other party, after the issuance of the attestation of attributes, to obtain data that allows transactions or user behaviour to be tracked, linked or correlated, or knowledge of transactions or user behaviour to be otherwise obtained, unless explicitly authorised by the user*". Although the EDIW Regulation does not expressly mention identity providers, the EDPS considers that the same limitation would also extend to identity providers (as "any other party").

20. Article 5a(16)(b) of the EDIW Regulation requires that the technical framework of the European Digital Identity Wallet "*enable[s] privacy preserving techniques which ensure unlinkability, where the attestation of attributes does not require the identification of the user.*" This unlinkability should prevent the identification of a user when the user needs to present some of their attributes to relying parties in the context of a transaction and identification is not necessary (e.g. to be authorised to the purchase of a product or service for adults only). The EDPS notes that the unlinkability should also apply:

    - among different transactions of the same user against the same relying party (when this is not necessary for the use-case);

    - between data held by the provider of personal identification data and attestation of attributes, on the one hand, and data held by the parties relying on those attributes, on the other hand.

21. Article 5b(3) of the EDIW Regulation provides that relying parties must not request users to provide any data other than indicated in Article 5b(2)(c) (i.e. the indication of the data to be requested by the relying party from users included in the registration of the relying party with the Member State where it is established).

2.1.2. The draft implementing regulation and data protection by design and by default

22. The EDPS considers that, in order to implement data protection by design and by default, the technical framework of the European Digital Identity Wallet should make reference to available 'state of the art' privacy-enhancing techniques (PETs) as mandatory measures. The EDPS recommends that the draft implementing regulation refers to the use of PETs and include specifications on when (for which specific aspects) and how these PETs must be implemented.

23. The EDPS considers that the ISO/IEC 18013-5 standard (on mobile driving licence), referred to in Annex I to the draft Implementing Regulation, may not appropriately support the privacy features of the European Digital Identity Wallet, in particular the requirement of unlinkability[14]. The EDPS thus recommends to further assess the available technical solutions and standards to ensure full compliance with the requirements of the EDIW Regulation and the requirements of data protection by design and by default.

24. The EDPS welcomes that requirements of the EDIW Regulation to ensure the integrity of the wallet, with a focus on cryptographic applications and material, their management and use, as well as the secure authentication of users and wallet integrity and authenticity management[15], have been referred to and implemented in the draft Implementing Regulation[16].

2.2. Specific comments

2.2.1. Transaction logs

25. The EDPS observes that the draft Implementing Regulation provides that the wallet units[17] shall log "at least" certain information on all transactions with wallet relying

[14] See in this regard also Baum et. al, "Cryptographers' Feedback on the EU Digital Identity's ARF", June 2024, p. 4. https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/issues/200

[15] Article 5a(4)(b) of the EDIW Regulation.

[16] Article 5 of the draft Implementing Regulation, 'Wallet secure cryptographic applications'.

[17] According to Article 2(2) of the draft Implementing Regulation, 'wallet unit' means a unique configuration of a wallet solution that includes wallet instances, wallet secure cryptographic applications and wallet secure cryptographic devices provided by a wallet provider to an individual wallet user.

parties[18] and other wallet units, including the personal data presented in the transaction[19]. The EDPS welcomes this provision, as it provides users[20] with an overview of their transactions, thereby upholding the data protection principle of transparency[21]. However, the EDPS recommends specifying in the draft Implementing Regulation a maximum storage period for transaction logs referred to in Article 9 of the draft implementing regulation.

2.2.2. Data recovery and portability

26. The EDPS notes that Article 13(1) of the draft implementing regulation provides that wallet solutions[22] must support the backup and recovery of wallet user data to enable migration to another wallet unit within the same wallet solution and electronic identification scheme. The data backed-up and restored must include the logs referred to in Article 9 of the draft implementing regulation, as well as any data needed to restore or re-issue person identification data and any electronic attestations of attributes to the new wallet unit. This function is needed to enable wallet users to request attestation providers[23] to re-issue the relevant data to another wallet unit, for example, making it possible to recover lost wallet units or to transfer information from one wallet provider to another to exercise the user's right to data portability[24]. The EDPS recommends that Article 13(1) of the draft implementing regulation specifies a maximum storage period for the back-up data, or at least specifies criteria that would allow to determine the appropriate storage duration.

2.2.3. Unlinkability

27. An important privacy-enhancing feature of the European Digital Identity Wallet consists in ensuring that the wallets are used without the user being trackable across different relying parties[25]. The technical infrastructure of the European Digital Identity Wallet should also be designed to ensure that only the minimal necessary

[18] According to Article 2(11) of the draft Implementing Regulation, 'wallet relying party' means a relying party that intends to rely upon wallet units for the provision of public or private services by means of digital interaction.
[19] Article 9(1)(c) of the draft Implementing Regulation.
[20] According to Article 2(1) of the draft Implementing Regulation, 'wallet user' means a natural or legal person who is the subject of the person identification data associated with the wallet unit that they are in control of.
[21] See also recital 9 of the draft Implementing Regulation.
[22] According to Article 2(3) of the draft Implementing Regulation, 'wallet solution' means a combination of software, hardware, services, settings, and configurations, including wallet instances, one or more wallet secure cryptographic applications and one or more wallet secure cryptographic devices, and which is managed and operated by a wallet provider.
[23] According to Article 2(7) of the draft Implementing Regulation, 'wallet provider' means a natural or legal person who provides wallet solutions.
[24] Recital 11 of the draft Implementing Regulation.
[25] Article 5a(16)(a) and recital (6) of the draft Implementing Regulation.

amount of data is transferred only to the authorised relying parties, while keeping the unlinkability between the different transactions. The draft implementing regulation should clearly and expressly refer to the unlinkability requirement and provide for appropriate specifications related to the implementation of this requirement[26].

2.2.4. Alternative identification and authentication means

28. The EDPS recalls that enjoyment of rights and access to services, particularly public services, as well as to employment or access to credit or other essential services, should not be restricted or hindered for persons not using the wallet. Where essential services are provided and access to those requires the use of the wallet, easily and promptly accessible alternatives (other identification and authentication means) must be offered by the service provider (as relying party). In other words, the use of the wallets must be optional, and in no circumstance create grounds for any type of discrimination. Natural persons should not suffer disadvantages for not using the wallet. The EDPS recommends that this important requirement of the EDIW Regulation[27] is fully taken into account also in the draft implementing regulation. For example, the draft implementing regulation could specify as functionality of the wallet that relying parties shall be able to provide information to the user of (at least some) alternative identification and authentication means when requesting access to the user to their wallet and require relying parties to provide such information.

2.2.5. Excessive access requests

29. The European Digital Identity Wallet is a system designed to store and/or provide access to a high quantity of and many different types of data, included personal data on the education, employment, health, of natural persons (as users). Article 5b(2)(c) of the EDIW Regulation provides that the relying party, at registration, must provide information on the intended use of the wallet, including "an indication of the data to be requested" from users. Article 5b(3) of the EDIW Regulation provides that relying parties must not request users to provide any data other than that indicated pursuant to Article 5(2)(c).

30. In this regard, the EDPS notes that the draft implementing regulation does not provide as functionality of the wallet the automated rejection of access requests by a relying party when the latter requests access for an intended use that has not been declared at registration and/or for types of data not indicated as object of the request

[26] In this regard, see also paragraph 23 of these formal comments.
[27] Article 5a(15) of the EDIW Regulation.

for the intended use at registration[28]. The EDPS considers that a functionality ensuring automated detection and blocking of excessive access requests might be useful addition in the future and should be considered.

31. However, to adequately address this issue, further work may also be necessary to develop harmonised specifications of data elements which are appropriate for certain intended use(s) (use-case(s)). The definition of the permissible attribute requests could not only address the legal certainty and interoperability issues, but also enhance user's control on their data and mitigate risks of 'request fatigue'.

Brussels,

[28] Such 'abusive' request by a relying party may include for instance the unnecessary request for generation of and access to pseudonyms to wallet units, that could be used to unnecessarily track users among different transactions.