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 person identification data and electronic attestations of attributes issued to 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 person identification data and electronic attestations of attributes issued to European Digital Identity Wallets ('the draft Implementing Regulation').
2. The draft Implementing Regulation is accompanied by an annex[2].
3. The objective of the draft is to lay down rules for the issuance of person identification data and electronic attestations of attributes to wallet units[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 an annex specifying the technical specifications for person identification data referred to in Article 3(3).
[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.

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,

[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.

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[9]. In particular the EDPS recommends making explicit reference to Regulation (EU) 2016/679 ('the GDPR')[10] and Directive 2002/58/EC ('ePrivacy Directive)[11].

11. The EDPS also 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.

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

12. The EDPS welcomes that the EDIW Regulation contains provisions[12] enabling the implementation of the wallet in accordance with the principle of data protection by design and by default[13]. 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*"[14]. 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] The EDPS notes that the accompanying Annex outlines the technical specifications for person identification data to be issued by providers of person identification data[9]. This person identification data must include certain mandatory attributes which constitute personal data: family name; given name; birth date; family name at birth; given name at birth; birth place; sex; nationality; issuance date of person identification data. Additionally, the person identification data may include optional attributes, which also constitute personal data, among which: age in years; birth country; resident address; personal administrative number; portrait (facial image of the wallet user) (Annex of the draft Implementing Regulation, Tables 1 and 2).

[10] 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.

[11] 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.

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

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

[14] 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).

2.1.4. The draft Implementing Regulation and data protection by design and by default

22. The EDPS considers that, 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[15].

2.2. Specific comments

2.2.1. Data minimisation

23. The EDPS recalls that the information contained in the person identification data and electronic attestations of attributes should be adequate, relevant and limited to what is necessary for the data's authentication and validation. In this respect, the EDPS recommends adding a specific reference, by way of a recital, to the data minimisation principle of the GDPR.

2.2.2. Personal administrative numbers

24. The EDPS also points out that the draft Implementing Regulation provides that Member States must ensure that the set of person identification data attributes issued to a given wallet user is unique[16]. It also envisages an optional attribute consisting in the "personal administrative number" which is "unique among all personal administrative numbers issued by the provider of person identification data"[17]. Due to its uniqueness, this attribute may involve the risk of becoming the default identifier for the purposes of authentication and validation, linking to all other

[15] See in particular paragraphs 26-30 below.
[16] Article 3(4) of the draft Implementing Regulation.
[17] Annex of the draft Implementing Regulation.

person identification data. The EDPS therefore welcomes the requirement, set out in the annex to the draft Implementing Regulation, according to which Member States (in case opt to include this attribute), must describe the policy applicable to the values of this attribute in their electronic identification schemes under which the person identification data is issued.

25. The EDPS considers that such policy should establish when (for which use cases) this optional attribute may be lawfully used by relying parties and provide for appropriate safeguards for the user, taking into account the risks to the rights and freedoms of the person concerned.

26. The EDPS recalls that, according to Article 87 GDPR, Member States may further determine the specific conditions for the processing of a national identification number or of any other identifier of general application. In that case, the identifier can only be used under appropriate safeguards for the rights and freedoms of the data subject, for instance clearly specifying the envisaged use cases of this identifier and restricting further use.

2.2.3. Revocation and validity status

27. The EDPS notes that draft Implementing Regulation provides for the possibility of revocation of person identification data and electronic attestations of attributes under specific circumstances[18]. The EDPS welcomes the requirement for providers of person identification data or electronic attestations of attributes to notify without delay the wallet users when their person identification data or electronic attestations of attributes are revoked, along with the reasons for the revocation[19]. However, the EDPS notes that it is equally important to ensure compliance with the principle of storage limitation. Revocation of data does not equate to its erasure. While revocation renders the data inactive, the data itself may still be stored. Therefore, the EDPS recommends specifying the maximum retention period of the person identification data (or electronic attestations of attributes) that have been revoked.

28. The draft Implementing Regulation provides that where providers of person identification data or electronic attestations of attributes revoke person identification data and electronic attestations of attributes issued to wallet units, they must make publicly available the validity status of person identification data or electronic attestations of attributes they issue and indicate the location of that information in the person identification data or electronic attestations of attributes[20]. The EDPS

[18] Article 5 of the draft Implementing Regulation.
[19] Article 5(3) of the draft Implementing Regulation.
[20] Article 5(6) of the draft Implementing Regulation.

emphasizes that while updated information about validity status is important, this publication should not reveal more person identification data or electronic attestations of attributes than necessary for the purpose of verifying validity.

29. The EDPS recalls that Article 5a(16) of the EDIW Regulation states 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. Having regard to the provisions on revocation in the second draft Implementing Regulation, the EDPS consider it necessary to address potential issues regarding unlinkability that may arise by the way relying parties check the validity of personal identification data or attestations of attributes.

2.2.3. Unlinkability

30. When relying parties verify at each transaction the validity status of personal identification data or attestations of attributes against an online resource, such access would reveal at least the online address of the relying party. This means that the party managing the online resource containing the revocation status could potentially learn from all the subsequent validity checks (who are) all the relying parties having access to the identification data or attributes they issue (for a given user).

31. To address this issue, the draft Implementing Regulation should aim to ensure unlinkability between the validity checks by the relying parties, on the one hand, and the information available to providers of identity data and of attestations of attributes or any other party tasked to operate the validity register, on the other hand. The EDPS recommends that the Commission further examine this issue and provides for adequate procedures and protocols to implement the requirement of unlinkability in the context of the draft Implementing Regulation.

Brussels, 30 September 2024

(e-signed)
Wojciech Rafał WIEWIÓROWSKI