EDPS Formal comments on the draft Commission Implementing Regulation laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and the Council as regards the certification 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 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and the Council as regards the certification 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 set out the general requirements applying to national certification schemes for the certification of wallet solutions, covering both functional and cybersecurity requirements, to the extent that cybersecurity certification schemes established pursuant to Regulation (EU) 2019/881 of the European Parliament and of the Council, do not, or only partially, cover those cybersecurity requirements[3].

[1] OJ L 295, 21.11.2018, p. 39.
[2] The draft Implementing Regulation is accompanied by nine annexes specifying the risk register for European Digital Identity Wallets, the criteria to assess the acceptability of assurance information, the functional requirements for wallet solutions, the methods and procedures for evaluation activities, the list of publicly available information about European Digital Identity Wallets, the methodology to assess the acceptability of assurance information, the content of the certificate of conformity, the content of the public certification report, and the certification assessment report and the schedule for mandatory surveillance evaluations.
[3] Recital 3 and Article 2(1) of the draft Implementing Regulation.

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

4. The draft Implementing Regulation is adopted pursuant to Article 5c(6) of Regulation (EU) No 910/2014[4], as amended by Regulation (EU) 2024/1183 amending 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.

---

[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.

[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. The EDPS notes the draft Implementing Regulation entails the processing of personal data. For instance, it is provided that national certification schemes must contain requirements for the applicant for certification to provide or otherwise make available to the certification body, among others, the information listed in Annex V to the draft Implementing Regulation[9]. This information includes the contact information of the wallet manufacturer or provider[10]. Additionally, with regard to the conformity assessment activities carried out by conformity assessment bodies, the draft Implementing Regulation provides that national certification schemes must contain methods and procedures to be used by the conformity assessment bodies when conducting their evaluation activities, which must include the elements set out in the accompanying Annex VI of the draft Implementing Regulation[11]. Some of these elements may constitute personal data, for instance: the name of the lead evaluator, if available; the evidence of the evaluator's competence (e.g. accreditation, personal certification, *etc.*) or evidence of the evaluator's impartiality (e.g. accreditation, etc.)[12].

11. Against this background, the EDPS suggests a recital referring to the applicability of the EU data protection legal framework (GDPR, as well as ePrivacy Directive) to the processing of personal data in the context of the draft Implementing Regulation.

12. The EDPS also notes the absence of the 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. Specific comments

13. The EDPS observes that the draft Implementing Regulation provides that the certification of wallets against data protection requirements is optional for Member States pursuant to Article 5c(5) of the EDIW Regulation. In other words, the draft Implementing Regulation does not specify requirements for certification pursuant to Regulation 2016/679[13]. Nevertheless, the EDPS considers that the certification of

[9] Article 7(6)(b) of the draft Implementing Regulation.
[10] See Annex V accompanying the draft Implementing Regulation, Article 1(d).
[11] Article 12(1)(f) of the draft Implementing Regulation.
[12] See Annex VI of the draft Implementing Regulation, Section 1(b).
[13] Recital 2 of the draft Implementing Regulation; Article 5c(5) of Regulation (EU) 910/2014 provides that "Compliance with the requirements set out in Article 5a of this Regulation related to the personal data processing operations may be certified pursuant to Regulation (EU) 2016/679."

wallets under Regulation 2016/679 should be promoted and be facilitated as much as possible by the draft Implementing Regulation.

14. In this context, the EDPS considers it useful to recall recital 27 of Regulation (EU) 2024/1183[14], which provides that by protecting users and companies from cybersecurity risks, the essential cybersecurity requirements laid down in that Regulation also contribute to enhancing the protection of personal data and privacy of individuals. It further indicates that "synergies on both standardisation and certification on cybersecurity aspects should be considered through the cooperation between the Commission, the European Standardisation Organizations, the European Union Agency for Cybersecurity (ENISA), the European Data Protection Board established by Regulation (EU) 2016/679 and the national data protection supervisory authorities."

15. The draft Implementing Regulation provides that the national certification schemes of wallet solutions must contain incident and vulnerability management requirements[15]: for instance, the obligation to notify to the certification bodies of any breach or compromise of the wallet solution or of the electronic identification scheme[16].

16. With regard to vulnerability notifications, the EDPS welcomes that the draft Implementing Regulation specifies that such notification requirement should not affect the criteria established by data protection legislation and/or Member States' data protection authorities for notification of personal data breaches[17]. However, the EDPS recommends making reference, in the draft Implementing Regulation, to the possible synergy between the mandatory notification of breach or compromise of the wallet solution and the policy, which must be established and implemented, and the notification of personal data breaches pursuant to the GDPR. Indeed, weaknesses in wallet implementations could easily result in significant personal data breaches.

17. The EDPS welcomes that the draft Implementing Regulation provides that, in order to avoid disclosure of person identification data and tracking activities back to the wallet user other than it is strictly necessary and intended by the user, the *wallet secure cryptographic application* ('WSCA') "can" adhere to privacy-by-design principles[18]. However, the EDPS recommends replacing "can" with "should".

[14] 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.
[15] Article 4(1) of the draft Implementing Regulation
[16] Article 4(2) of the draft Implementing Regulation.
[17] Recital 16 of the draft Implementing Regulation.
[18] Recital 8 of the draft Implementing Regulation.

18. The EDPS also notes that the draft Implementing Regulation states that national certification schemes must contain requirements for certification bodies concerning a record system for all relevant information produced in connection with the conformity assessment activities that they perform, included data issued and received by wallet providers and by the electronic identification schemes under which the wallets are provided. The records may be kept electronically and must remain accessible for as long as required by Union law or national law, and for at least five years after the cancellation or expiry of the relevant certificate of conformity[19]. In addition, national certification schemes must set out the requirements for the holder of the certificate of conformity to store, for instance, records of the information provided to the certification body, securely for the purpose of this Regulation, for at least five years after the cancellation or expiry of the relevant certificate of conformity[20]. Since, as already indicated, certain data provided to certification bodies may constitute personal data, the EDPS recommends specifying the maximum retention period - in addition to the minimum retention period (indicated as "at least") - for these data.

Brussels,

[19] Article 18(1) of the draft Implementing Regulation.
[20] Article 18(2) of the draft Implementing Regulation.