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 of the Council as regards reactions to security breaches 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 10 December 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[2] as regards reactions to security breaches of European Digital Identity Wallets (EUDIWs) ('the draft implementing regulation').
2. The objective of the draft implementing regulation is to lay down rules for reactions to security breaches of the wallets, to be updated on a regular basis to keep in line with technology and standards developments and with the work carried out on the basis of Commission Recommendation (EU) 2021/946[3], and in particular the Architecture and Reference Framework[4].
3. The draft implementing regulation is adopted pursuant to Article 5e(5) of Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[1] OJ L 295, 21.11.2018, p. 39.
[2] 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).
[3] Commission Recommendation (EU) 2021/946 of 3 June 2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework, C/2021/3968 (OJ L 210, 14.6.2021, p. 51–54).
[4] Article 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 EDPS previously issued 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[5].

5. 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. The EDPS welcomes the reference to this consultation in Recital 12 of the draft implementing regulation.

6. These formal comments 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[6].

7. 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

8. The EDPS welcomes recital 2 of the draft implementing regulation, confirming that Regulation (EU) 2016/679[7] ('GDPR') and, where relevant, Directive 2002/58/EC[8] apply to the personal data processing activities under the draft implementing regulation. However, since the Commission might process personal data in the context of notifications pursuant to Articles 3(3), 5, 7 and 9 of the draft implementing regulation, the EDPS recommends adding in this recital of the draft implementing regulation a reference to the applicability of the EUDPR in case of processing of personal data by the Commission.

9. The EDPS recommends recalling in a recital of the draft implementing regulation that the rules on assessment and notification of a security breach it contains are without prejudice to the obligations to notify personal data breaches to the data protection

[5] 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, issued on 28 July 2021.
[6] 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.
[7] Regulation (EU) No 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) (Text with EEA relevance) (OJ L 119, 4.5.2016, p. 1).
[8] 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).

supervisory authority (Article 33 GDPR) and, where relevant, to communicate the personal data breach to the data subject (Article 34 GDPR).

10. The EDPS recalls that Article 46a(4)(g) of Regulation (EU) No 910/2014 requires the supervisory bodies established under the European Digital Identity Wallet framework "*to cooperate with competent supervisory authorities established pursuant to Article 51 of Regulation (EU) 2016/679, in particular, by informing them without undue delay, where personal data protection rules appear to have been infringed and about security breaches which appear to constitute personal data breaches.*"

11. Articles 5[9], 7[10] and 9[11] of the draft implementing regulation require Member States to inform users and notify the national single points of contact[12] and the Commission in case of suspension of the provision and use of EUDIW solutions following a security breach, re-establishment of a EUDIW solution, or withdrawal a EUDIW solution following a severe security breach or compromise. The EDPS recommends requiring Member States to ensure that data protection supervisory authorities are also informed of such events without undue delay, in accordance with Article 46a(4)(g) of Regulation (EU) No 910/2014. This would enable data protection authorities to effectively ensure the protection of personal data that, in most cases, might be at stake in case security breach as defined in the draft implementing regulation.

12. The EDPS notes that Article 5(3) of the draft implementing regulation establishes the minimum information to be included in the suspension notifications. However, Article 5 does not specify the information to be provided to the affected wallet users or relying parties. The EDPS therefore recommends specifying in Article 5 of the draft implementing regulation the minimum information to be provided to the affected wallet users and relying parties.

13. The same consideration applies to Article 9 of the draft implementing regulation, related to notifications of withdrawal of wallet solutions. Also in this case, the provisions refer to the content of the 'withdrawal notifications'[13], but not to the content of the information to be provided to the affected users and relying parties. The EDPS therefore recommends specifying in Article 9 of the draft implementing regulation the information to be provided to affected users and relying parties in case of withdrawal of the wallet solution.

14. The EDPS considers that information to be provided to users pursuant to Articles 5 and 9, as well as pursuant to Article 7 of the draft implementing regulation, should contain, in particular and where relevant, indication of measures that users can take

[9] Article 5 of the draft implementing regulation on notifications about suspensions and remedies.
[10] Article 7 of the draft implementing regulation on re-establishment notifications.
[11] Article 9 of the draft implementing regulation on withdrawal notifications.
[12] designated pursuant to Article 46c(1) of Regulation (EU) No 910/2014.
[13] Article 9(3) of the draft implementing regulation.

to mitigate the possible impact of the breach, as well as the contact details (at least phone number and e-mail address) of the wallet solution providers.

15. Regarding Annex I of the draft implementing regulation, the EDPS recommends expanding the criterion under letter (g), which refer refers to the likeliness "to affect personal data as defined in Article 9(1) and 10 of the GDPR" as one of the (sub)criteria for the assessment of a security breach or compromise.[14] In particular, the EDPS recommends expanding this criterion by referring to "*personal data whose breach may negatively affect the person concerned and, in particular, in case of breach of personal data as defined in Article 9(1) and 10 of the GDPR*". This is due to the fact that also personal data, which are not special categories of personal data, for instance credit or debit card data, can nonetheless warrant the measures required by the draft implementing regulation in case of security breach or compromise of the wallet solution.

Brussels, 31 January 2025

(e-signed)
Wojciech Rafał WIEWIÓROWSKI

[14] Annex I, point 1, letter (g) refers to the likeliness *"to affect personal data as defined in Article 9(1) and 10 of the GDPR".*