



2024/2980

4.12.2024

COMMISSION IMPLEMENTING REGULATION (EU) 2024/2980

of 28 November 2024

laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards notifications to the Commission concerning the European Digital Identity Wallet ecosystem

THE EUROPEAN COMMISSION,

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

Having regard to 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 ⁽¹⁾, and in particular Article 5a(23) thereof,

Whereas:

- (1) The European Digital Identity Framework established by Regulation (EU) No 910/2014 is a crucial component in the establishment of a secure and interoperable digital identity ecosystem across the Union. With the European Digital Identity Wallets ('wallets') being the cornerstone of the framework, it aims at facilitating access to services across Member States, while ensuring the protection of personal data and privacy.
- (2) Regulation (EU) 2016/679 of the European Parliament and of the Council ⁽²⁾, or Regulation (EU) 2018/1725 of the European Parliament and of the Council ⁽³⁾ and, where relevant, Directive 2002/58/EC of the European Parliament and of the Council ⁽⁴⁾ apply to all personal data processing activities under this Regulation.
- (3) Article 5a(23) of Regulation (EU) No 910/2014 mandates the Commission, where necessary, to establish relevant specifications and procedures. This is achieved by means of four Implementing Regulations, dealing with protocols and interfaces: Commission Implementing Regulation (EU) 2024/2982 ⁽⁵⁾, integrity and core functionalities: Commission Implementing Regulation (EU) 2024/2979 ⁽⁶⁾, person identification data and electronic attestation of attributes: Commission Implementing Regulation (EU) 2024/2977 ⁽⁷⁾, as well as the notifications to the Commission: Commission Implementing Regulation (EU) 2024/2980 ⁽⁸⁾. This Regulation lays down the relevant requirements for Member States' notifications of trusted entities that establish trustworthiness of the European Digital Identity Framework.

⁽¹⁾ OJ L 257, 28.8.2014, p. 73, ELI: <http://data.europa.eu/eli/reg/2014/910/oj>.

⁽²⁾ 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, ELI: <http://data.europa.eu/eli/reg/2016/679/oj>).

⁽³⁾ 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 L 295, 21.11.2018, p. 39, ELI: <http://data.europa.eu/eli/reg/2018/1725/oj>).

⁽⁴⁾ 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, ELI: <http://data.europa.eu/eli/dir/2002/58/oj>).

⁽⁵⁾ Commission Implementing Regulation (EU) 2024/2982 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards protocols and interfaces to be supported by the European Digital Identity Framework (OJ L, 2024/2982, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

⁽⁶⁾ Commission Implementing Regulation (EU) 2024/2979 of 28 November 2024 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 (OJ L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

⁽⁷⁾ Commission Implementing Regulation (EU) 2024/2977 of 28 November 2024 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 (OJ L, 2024/2977, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).

⁽⁸⁾ Commission Implementing Regulation (EU) 2024/2980 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards notifications to the Commission concerning the European Digital Identity Wallet ecosystem (OJ L, 2024/2980, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2980/oj).

- (4) The Commission regularly assesses new technologies, practices, standards or technical specifications. To ensure the highest level of harmonisation among Member States for the development and certification of the wallets, the technical specifications set out in this Regulation rely on the work carried out on the basis of Commission Recommendation (EU) 2021/946 of 3 June 2021 on a common Union Toolbox for a coordinated approach towards a European Digital Framework⁽⁹⁾ and in particular the architecture and reference framework. In accordance with Recital 75 of Regulation (EU) 2024/1183 of the European Parliament and of the Council⁽¹⁰⁾, the Commission should review and update this Implementing Regulation, if necessary, to keep it in line with global developments, the architecture and reference framework, and to follow the best practices on the internal market.
- (5) To meet the objective of establishing a transparent and reliable source of information for authenticating entities in the European Digital Identity Wallet ecosystem, such as wallet providers, providers of person identification data and wallet-relying parties, Member States should notify the required information to the electronic system provided by the Commission. In line with the approach taken by Commission Implementing Decision (EU) 2015/1984⁽¹¹⁾ defining the circumstances, formats and procedures of notification with respect to electronic identification schemes applicable to electronic identification means, information should be provided by the Member States to the Commission in English. In this manner, descriptions of electronic identification schemes are available in English for all such schemes, irrespective of whether they relate to electronic identification means or to wallets.
- (6) For the same objective of establishing information sources that enable the authentication of entities in the European Digital Identity Wallet ecosystem, the Commission should establish an infrastructure to make the information available to the public in a secure, human-readable, clear, and easily accessible manner, as well as in an electronically signed or sealed form suitable for automated processing, including by offering an application programming interface.
- (7) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725, and delivered its opinion on 30 September 2024.
- (8) The measures provided for in this Regulation are in accordance with the opinion of the Committee referred to in Article 48 of Regulation (EU) No 910/2014,

HAS ADOPTED THIS REGULATION:

Article 1

Subject matter and scope

This Regulation establishes obligations in relation to notifications that enable the validation of:

- (1) the electronic registers used by a Member State to publish information on wallet-relying parties registered in that Member State in accordance with Article 5b(5) of Regulation (EU) No 910/2014 ('registers of wallet-relying parties'), the location of the registers of wallet-relying parties, and the identification of the registrars of wallet-relying parties;
- (2) the identity of the registered wallet-relying parties;
- (3) the authenticity and validity of wallet units;
- (4) the identification of the wallet providers;

⁽⁹⁾ OJ L 210, 14.6.2021, p. 51, ELI: <http://data.europa.eu/eli/reco/2021/946/oj>.

⁽¹⁰⁾ 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, ELI: <http://data.europa.eu/eli/reg/2024/1183/oj>).

⁽¹¹⁾ Commission Implementing Decision (EU) 2015/1984 of 3 November 2015 defining the circumstances, formats and procedures of notification pursuant to Article 9(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (OJ L 289, 5.11.2015, p. 18, ELI: http://data.europa.eu/eli/dec_impl/2015/1984/oj).

- (5) the authenticity of person identification data;
- (6) the identification of the providers of person identification data;

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 Recommendation (EU) 2021/946, and in particular the architecture and reference framework.

Article 2

Definitions

For the purpose of this Regulation, the following definitions apply:

- (1) 'wallet provider' means a natural or legal person who provides wallet solutions;
- (2) 'provider of person identification data' means a natural or legal person responsible for issuing and revoking the person identification data and ensuring that the person identification data of a user is cryptographically bound to a wallet unit;
- (3) '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;
- (4) 'register of wallet-relying parties' means an electronic register used by a Member State to make information on wallet-relying parties registered in that Member State publicly available as set out in Article 5b(5) of Regulation (EU) No 910/2014;
- (5) 'registrar of wallet-relying parties' means the body responsible for establishing and maintaining the list of registered wallet-relying parties established in their territory who has been designated by a Member State;
- (6) '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;
- (7) '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;
- (8) 'wallet instance' means the application installed and configured on a wallet user's device or environment, which is part of a wallet unit, and that the wallet user uses to interact with the wallet unit;
- (9) 'wallet secure cryptographic application' means an application that manages critical assets by being linked to and using the cryptographic and non-cryptographic functions provided by the wallet secure cryptographic device;
- (10) 'wallet secure cryptographic device' means a tamper-resistant device that provides an environment that is linked to and used by the wallet secure cryptographic application to protect critical assets and provide cryptographic functions for the secure execution of critical operations;
- (11) 'critical assets' means assets within or in relation to a wallet unit of such extraordinary importance that where their availability, confidentiality or integrity are compromised, this would have a very serious, debilitating effect on the ability to rely on the wallet unit;
- (12) 'wallet user' means a user who is in control of the wallet unit;
- (13) 'provider of wallet-relying party access certificates' means a natural or legal person mandated by a Member State to issue relying party access certificates to wallet-relying parties registered in that Member State;
- (14) 'wallet-relying party access certificate' means a certificate for electronic seals or signatures authenticating and validating the wallet-relying party issued by a provider of wallet-relying party access certificates.

*Article 3***Notification system**

1. The Commission shall make available to Member States a secure electronic notification system, no later than twelve months after the publication of this Regulation in the *Official Journal of the European Union*, enabling Member States to notify the information on the bodies and mechanisms referred to in Article 5a(18) of Regulation (EU) No 910/2014.
2. The secure electronic notification system shall comply with the technical requirements laid down in Annex I.

*Article 4***Notifications by Member States**

1. Member States shall submit, through the secure electronic notification system referred to in Article 3(1), at least the information specified in Annex II.
2. Member States shall make the notifications at least in English. Member States shall not be obliged to translate any document supporting the notifications where this would create an unreasonable administrative or financial burden.
3. The Commission may request additional information or clarifications from the Member States for the purpose of verifying the completeness and consistency of the notified information.

*Article 5***Publications by the Commission**

1. The Commission shall establish, maintain and publish a list compiling the information notified by Member States on registrars of wallet-relying parties and registers of wallet-relying parties as referred to in Annex II section 1.
2. The Commission shall establish, maintain and publish a list compiling the information notified by Member States on wallet providers, providers of person identification data and providers of wallet-relying party access certificates, as referred to in Annex II sections 2, 3 and 4.
3. The Commission shall ensure the lists referred to in paragraphs 1 and 2 of this Article can be accessed:
 - (a) in both electronically signed or sealed form suitable for automated processing and through a human readable website available in at least English;
 - (b) without the need to register or to be authenticated to obtain or read the lists;
 - (c) securely by using state of the art transport layer encryption.
4. In addition to the publications of the lists referred to in paragraphs 1 and 2, the Commission shall publish:
 - (a) the technical specifications the Commission uses for the structure of the lists;
 - (b) the details of the URL where the lists are published;
 - (c) the certificates to be used to verify the signature or seal on the lists;
 - (d) the details on mechanisms used to validate changes to the location referred to in point (b) or to the certificates referred to in point (c).

*Article 6***Entry into force**

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 28 November 2024.

For the Commission
The President
Ursula VON DER LEYEN

ANNEX I

REQUIREMENTS FOR THE COMMISSION'S NOTIFICATIONS SYSTEM

1. The interface of the secure electronic notifications system shall be at least in English.
 2. The secure electronic notifications system provided by the Commission shall be designed to:
 - (a) allow the Member States to submit the same information only once, by re-using prior submitted information where appropriate;
 - (b) enable the submission of information via both machine processable interfaces and human usable interfaces;
 - (c) support appropriate access controls and access control management, delegating to the Member States the power to grant access to competent representatives as regards the notifications;
 - (d) support notifications of the information specified in Annex II;
 - (e) allow Member States to view notified information;
 - (f) acknowledge receipt of notifications of information by electronic means;
 - (g) retain, and allow Member States to view, a historical record of any changes in any notified information.
-

ANNEX II

REQUIREMENTS FOR MEMBER STATES' NOTIFICATIONS**1. Notifications of information on registrars and registers**

- (1) Member States shall provide the following information to the Commission on their registrars and registers:
 - (a) the name of the register;
 - (b) at least one URL where the register is available for access, which shall use state of the art transport layer encryption;
 - (c) the name of the registrar that is responsible for that register;
 - (d) where applicable, the registration number of the registrar;
 - (e) the Member State in which the registrar is established;
 - (f) the contact email and contact phone number of the registrar, for matters related to the register;
 - (g) where applicable, the URL of a webpage for additional information about the registrar and the register;
 - (h) the URL of the webpage where the registration policy that applies to the register and related information are located;
 - (i) one or more certificates compliant with IETF RFC 3647 which can be used to verify the signature or seal created by the registrar on the register data and for which the certified identity data include the name of the registrar, and where applicable, the registration number of the registrar, as provided in points (c) and (d), respectively.
- (2) That information referred to in point (1) shall be provided per register and registrar.

2. Notifications of information on wallet providers and on the mechanisms by which to validate the authenticity and validity of wallet units

- (1) Member States shall provide the following information to the Commission on wallet providers:
 - (a) the name of the wallet provider;
 - (b) where applicable, the registration number of the wallet provider;
 - (c) where applicable, the name of the body responsible for the provision of the wallet solution;
 - (d) the Member State in which the wallet provider is established;
 - (e) the contact email and contact phone number of the wallet provider, for matters related to the wallet solutions it provides;
 - (f) where applicable, the URL of the webpage for additional information about the wallet provider and the wallet solution;
 - (g) the URL of the webpage where the policies, terms and conditions of the wallet provider that apply to the provision and use of the wallet solution it provides are located;
 - (h) one or more certificates compliant with IETF RFC 3647 that can be used to authenticate and validate the components of the wallet unit the wallet provides, and for which the certified identity data includes the name, and where applicable, the registration number of the wallet provider, as specified in points (a) and (b), respectively;
 - (i) for each wallet solution provided by the wallet provider, the name and the reference number of the wallet solution it provides, as the Commission shall publish this information in the *Official Journal of the European Union* pursuant to Article 5d of Regulation (EU) No 910/2014.
- (2) That information referred to in point (1) shall be provided per provider.

3. Notifications of information on providers of person identification data and on the mechanisms enabling the authentication and validation of person identification data

- (1) Member States shall provide the following information to the Commission on providers of person identification data:
- (a) the name of the provider of person identification data;
 - (b) where applicable, a registration number of the provider of person identification data;
 - (c) where applicable, the name of the body responsible for ensuring that the person identification data is associated with the wallet unit;
 - (d) the Member State in which the provider of person identification data is established;
 - (e) the contact email and contact phone number of the provider of person identification data, for matters related to the person identification data it provides;
 - (f) where applicable, the URL of the webpage that contains additional information about the person identification data provider;
 - (g) the URL of the webpage that contains the policies, terms and conditions of the provider of person identification data that apply to the provision and use of the person identification data it provides;
 - (h) one or more certificates compliant with IETF RFC 3647 that can be used to verify the signature or seal created by the provider of person identification data on the person identification data it provides, and for which the certified identity data include the name, and where applicable, the registration number of the person identification data provider, as specified in points (a) and (b), respectively.
- (2) That information referred to in point (1) shall be provided per provider.

4. Notifications of information on providers of wallet-relying party access certificates

- (1) Member States shall provide the following information to the Commission on providers of wallet-relying party access certificates:
- (a) the name of the provider of wallet-relying party access certificates;
 - (b) where applicable, a registration number of the provider of wallet-relying party access certificates;
 - (c) the Member State in which the provider of wallet-relying party access certificates is established;
 - (d) the contact email and contact phone number of the provider of wallet-relying party access certificates, for matters related to the access certificates it provides to wallet-relying parties;
 - (e) where applicable, the URL of the webpage of the provider of wallet-relying party access certificates that contains additional information about the provider and the access certificates it provides to wallet-relying parties;
 - (f) the URL of the webpage that contains the policies, terms and conditions that apply to the provision and use of the access certificates it provides to wallet-relying parties;
 - (g) one or more certificates compliant with IETF RFC 3647 that can be used to verify the signature or seal created by the provider of wallet-relying party access certificates on the access certificate it provides to wallet-relying parties, with, where applicable, the information required to distinguish wallet-relying party access certificates from other certificates.
- (2) The information referred to in point (1) shall be provided per provider of wallet-relying party access certificates.