Official Journal
of the European Union

EN
L series

2024/2977

4.12.2024

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

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') as 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]) and, where relevant, Directive 2002/58/EC of the European Parliament and of the Council ([3]) 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 the relevant specifications and procedures. This is achieved by means of four Implementing Regulations, dealing with protocols and interfaces: Commission Implementing Regulation (EU) 2024/2982 ([4]), integrity and core functionalities: Commission Implementing Regulation (EU) 2024/2979 ([5]), person identification data and electronic attestation of attributes: Commission Implementing Regulation (EU) 2024/2977 ([6]), as well as the notifications to the Commission: Commission Implementing Regulation (EU) 2024/2980 ([7]). This Regulation lays down the relevant requirements for person identification data and electronic attestations of attributes to be issued to European Digital Identity Wallets.

([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]) 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).

([4]) 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).

([5]) 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).

([6]) 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).

([7]) 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 Implementing 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 Identity Framework ([8]) and in particular the architecture and reference framework which is part of it. In accordance with Recital 75 of Regulation (EU) 2024/1183 of the European Parliament and of the Council ([9]), 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 ensure data protection by design and by default, the wallets should be provided with several privacy enhancing features to prevent providers of electronic identification means and electronic attestation of attributes from combining personal data obtained when providing other services with the personal data processed to provide the services falling within the scope of Regulation (EU) No 910/2014.

(6) To ensure harmonisation, certain common functionalities should be available in all wallets, including the ability to securely request, obtain, select, combine, store, delete, share, and present, under the sole control of the wallet user, person identification data and electronic attestations of attributes. To ensure that person identification data and electronic attestations of attributes can be processed via every wallet unit, technical specifications concerning person identification data attributes, the data format, and the infrastructure required to ensure appropriate trustworthiness of person identification data need to be supported by all wallet solutions. Further, common specifications in relation to attributes of person identification data aim at ensuring that this data can be used for identity matching as required.

(7) Member States are to ensure that the wallets are able to authenticate relying parties, providers of person identification data and providers of electronic attestations of attributes irrespective of where they are established in the Union. To achieve this, these entities should use wallet-relying party access certificates when they identify themselves to wallet units. To guarantee interoperability of these certificates across all wallets provided within the Union, wallet-relying parties' access certificates should adhere to common standards. The Commission, in collaboration with Member States, should closely monitor the development of new or alternative standards on which relying-party access certificates could be built. In particular, trust models that have proven their efficacy and security in Member States should be assessed.

(8) To ensure transparency towards wallet users, Member States should publish information indicating which wallet solutions are supported by providers of person identification data established in their territories. Since the identity of the user must be as reliable as possible, a common assurance level high should be imposed on the identity proofing of wallet users prior to the issuance of person identification data, according to assurance level high as laid down for electronic identification means under Regulation (EU) No 910/2014. In this manner, the wallet units ensure the highest available degree of trustworthiness for means of identification across the Union. During enrolment of wallet users at level of assurance high, various secure processes are possible, for instance, where the wallet user has been verified to be in possession of photo or biometric identification evidence recognised but not issued by the Member State in which the application for the electronic identification means is made and that evidence represents the claimed identity, the evidence should be checked to determine that it is valid according to a relevant authoritative source.

(9) In order to support interoperability, electronic attestations of attributes should comply with harmonised requirements on the format.

(10) To protect the data of wallet users and to ensure the authenticity of electronic attestations of attributes, mechanisms for the authentication of providers of electronic attestations of attributes, and for the verification of the authenticity and validity of wallet units by that provider should apply prior to the issuance of the attestations to wallet units.

([8]) OJ L 210, 14.6.2021, p. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj.

([9]) 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) In order to avoid the use of, and the reliance on, person identification data and electronic attestations of attributes that have lost their legal validity after being issued to a wallet unit, providers of person identification data and of electronic attestations of attributes should publish a policy outlining the circumstances and procedures for revocation.

(12) To ensure that the person identification data uniquely represents the wallet user, Member States should, in addition to the mandatory attributes in the person identification data set out in this Regulation, provide optional attributes needed to ensure that the set of person identification data is unique.

(13) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council [10] and delivered its opinion on 30 September 2024.

(14) 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 lays down rules for the issuance of person identification data and electronic attestations of attributes to wallet units, 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 user' means a user who is in control of the wallet unit;

(2) '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;

(3) '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;

(4) '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;

(5) 'wallet unit attestation' means a data object that describes the components of the wallet unit or allows authentication and validation of those components;

(6) '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;

(7) '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] 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).

(8) '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;

(9) 'wallet provider' means a natural or legal person who provides wallet solutions;

(10) '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;

(11) '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;

(12) '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;

(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.

Article 3

Issuance of person identification data to wallet units

1. Providers of person identification data shall issue person identification data to wallet units in accordance with the electronic identification schemes under which wallet solutions are provided.

2. Providers of person identification data shall ensure that person identification data issued to wallet units contains the information necessary for authentication and validation of the person identification data.

3. Providers of person identification data shall ensure that person identification data issued to wallet units comply with the technical specifications set out in the Annex.

4. Member States shall ensure that the person identification data issued to a given wallet user is unique for the Member State.

5. Providers of person identification data shall ensure that person identification data that they issue is cryptographically bound to the wallet unit to which it is issued.

6. Member States shall make publicly available a list of wallet solutions that are supported by providers of person identification data that is part of electronic identification schemes of that Member State.

7. Member States shall enroll wallet users in accordance with the requirements relating to enrolment at assurance level high, as set out in Commission Implementing Regulation (EU) 2015/1502 ([11]). In the context of the enrolment process, providers of person identification data shall perform identity verification of the wallet user in accordance with the requirements related to identity proofing and verification before issuing the person identification data to the wallet unit of the corresponding wallet user.

8. When issuing person identification data to wallet units, providers of person identification data shall identify themselves to wallet units using their wallet-relying party access certificate or by using another authentication mechanism in accordance with an electronic identity scheme notified at assurance level high.

([11]) Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) 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 235, 9.9.2015, p. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

9. Before issuing person identification data to a wallet unit, providers of person identification data shall authenticate and validate the wallet unit attestation of the wallet unit and verify that the wallet unit belongs to a wallet solution the provider of person identification data accepts or use another authentication mechanism in accordance with an electronic identity scheme notified at assurance level high.

Article 4

Issuance of electronic attestations of attributes to wallet units

1. Electronic attestations of attributes issued to wallet units shall comply with at least one of the standards in the list set out in Annex I of Implementing Regulation (EU) 2024/2979.

2. Providers of electronic attestations of attributes shall identify themselves to wallet units using their wallet-relying party access certificate.

3. Providers of electronic attestations of attributes shall ensure that electronic attestations of attributes issued to wallet units contain the information necessary for authentication and validation of those electronic attestations of attributes.

Article 5

Revocation of person identification data

1. Providers of person identification data issued to a wallet unit shall have written and publicly accessible policies relating to validity status management, including, where applicable, the conditions under which such person identification data can be revoked without delay.

2. Only providers of person identification data or electronic attestation of attributes can revoke the person identification data or electronic attestations of attributes issued by them.

3. Where providers of person identification data have revoked person identification data, they shall, through dedicated and secure channels, inform wallet users subject of those person identification data within 24 hours of the revocation and of the reasons for the revocation. This shall be done in a manner that is concise, easily accessible and using clear and plain language.

4. Where providers of person identification data revoke person identification data issued to wallet units, they shall do so in each of the following circumstances:

(a) upon the explicit request of the wallet user to whose wallet unit the person identification data or electronic attestation of attributes were issued to;

(b) where the wallet unit attestation to which the person identification data was issued to has been revoked;

(c) in other situations determined by the providers of person identification data or electronic attestations of attributes in their policies referred to in paragraph 1.

5. Providers of person identification data issued to a wallet unit shall ensure that revocations cannot be reverted.

6. The revoked person identification data shall remain accessible for as long as required by Union law or national law.

7. Where providers of person identification data revoke person identification data issued to wallet units, they shall make publicly available the validity status of person identification data they issue, in a privacy preserving manner, and indicate the location of that information in the person identification data.

8. Providers of person identification data shall enable privacy preserving techniques which ensure unlinkability where the electronic attestations of attributes do not require the identification of the user.

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

TECHNICAL SPECIFICATIONS FOR PERSON IDENTIFICATION DATA REFERRED TO IN ARTICLE 3(3)

1. **Set of natural person identification data**

Table 1

Mandatory person identification data for the natural person

Data identifier	Definition	Presence
family_name	Current last name(s) or surname(s) of the user to whom the person identification data relates.	mandatory
given_name	Current first name(s), including middle name(s) where applicable, of the user to whom the person identification data relates.	mandatory
birth_date	Day, month, and year on which the user to whom the person identification data relates was born.	mandatory
birth_place	The country as an alpha-2 country code as specified in ISO 3166-1, or the state, province, district, or local area or the municipality, city, town, or village where the user to whom the person identification data relates was born.	mandatory
nationality	One or more alpha-2 country codes as specified in ISO 3166-1, representing the nationality of the user to whom the person identification data relates.	mandatory

Where an attribute value is not known for the person or cannot otherwise be issued as part of the person identification dataset, Member States shall use an attribute value appropriate to the situation instead.

Table 2

Optional person identification data for the natural person

Data identifier	Definition	Presence
resident_address	The full address of the place where the user to whom the person identification data relates currently resides or can be contacted (street name, house number, city etc.).	optional
resident_country	The country where the user to whom the person identification data relates currently resides, as an alpha-2 country code as specified in ISO 3166-1.	optional
resident_state	The state, province, district, or local area where the user to whom the person identification data relates currently resides.	optional

Data identifier	Definition	Presence
resident_city	The municipality, city, town, or village where the user to whom the person identification data relates currently resides.	optional
resident_postal_code	The postal code of the place where the user to whom the person identification data relates currently resides.	optional
resident_street	The name of the street where the user to whom the person identification data relates currently resides.	optional
resident_house_number	The house number where the user to whom the person identification data relates currently resides, including any affix or suffix.	optional
personal_administrative_number	A value assigned to the natural person that is unique among all personal administrative numbers issued by the provider of person identification data. Where Member States opt to include this attribute, they shall describe in their electronic identification schemes under which the person identification data is issued, the policy that they apply to the values of this attribute, including, where applicable, specific conditions for the processing of this value.	optional
portrait	Facial image of the wallet user compliant with ISO 19794-5 or ISO 39794 specifications.	optional
family_name_birth	Last name(s) or surname(s) of the person identification data user at the time of birth.	optional
given_name_birth	First name(s), including middle name(s), of the person identification data user at the time of birth.	optional
sex	Values shall be one of the following: 0 = not known; 1 = male; 2 = female; 3 = other; 4 = inter; 5 = diverse; 6 = open; 9 = not applicable. For values 0, 1, 2 and 9, ISO/IEC 5218 applies.	optional
email_address	Electronic mail address of the user to whom the person identification data relates [in conformance with RFC 5322].	optional
mobile_phone_number	Mobile telephone number of the user to whom the person identification data relates, starting with the '+' symbol as the international code prefix and the country code, followed by numbers only.	optional

2. **Set of legal person identification data**

Table 3

Mandatory person identification data for the legal person

Data element	Presence
current legal name	mandatory
a unique identifier constructed by the sending Member State in accordance with the technical specifications for the purposes of cross-border identification and which is as persistent as possible in time	mandatory

Where a data element is not known for the person or cannot otherwise be issued as part of the person identification dataset, Member States shall use an attribute value appropriate to the situation instead.

Table 4

Optional person identification data for the legal person

Data element	Presence
current address	optional
VAT registration number	optional
tax reference number	optional
European unique identifier referred to in Directive (EU) 2017/1132 of the European Parliament and of the Council	optional
Legal Entity Identifier (LEI) referred to in Commission Implementing Regulation (EU) 2022/1860	optional
Economic Operator Registration and Identification (EORI) referred to in Commission Implementing Regulation (EU) No 1352/2013	optional
excise number provided in Article 2(12) of Council Regulation (EU) No 389/2012	optional

3. **Set of metadata about person identification data**

Table 5

Metadata about the person identification data

Data identifier	Definition	Presence
expiry_date	Date (and if possible time) when the person identification data will expire.	mandatory
issuing_authority	Name of the administrative authority that issued the person identification data, or the ISO 3166 alpha-2 country code of the respective Member State if there is no separate authority entitled to issue person identification data.	mandatory
issuing_country	Alpha-2 country code, as specified in ISO 3166-1, of the country or territory of the provider of the person identification data.	mandatory

Data identifier	Definition	Presence
document_number	A number for the person identification data, assigned by the provider of person identification data.	optional
issuing_jurisdiction	Country subdivision code of the jurisdiction that issued the person identification data, as specified in ISO 3166-2:2020, Clause 8. The first part of the code shall be the same as the value for the issuing country.	optional
location_status	The location of validity status information on the person identification data where the providers of person identification data revoke person identification data.	optional

4. **Encoding of person identification data attributes**

Person identification data shall be issued in two formats:

(1) the format specified in ISO/IEC 18013-5:2021;

(2) 'Verifiable Credentials Data Model 1.1.', W3C Recommendation, 3 March 2022.

5. **Trust infrastructure details**

The list of providers of person identification data made available by the Commission in accordance with Implementing Regulation (EU) 2024/2980 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 as regards notifications shall enable authentication of person identification data.