►B 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)

Amended by:

		Official Journal		
		No	page	date
►M1	Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022	L 333	80	27.12.2022
►M2	Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024	L 1183	1	30.4.2024

▼B

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

CHAPTER I

GENERAL PROVISIONS

▼M2

Article 1

Subject matter

This Regulation aims to ensure the proper functioning of the internal market and the provision of an adequate level of security of electronic identification means and trust services used across the Union, in order to enable and facilitate the exercise by natural and legal persons of the right to participate in digital society safely and to access online public and private services throughout the Union. For those purposes, this Regulation:

(a) lays down the conditions under which Member States are to recognise natural and legal persons' electronic identification means falling under a notified electronic identification scheme of another Member State and provide and recognise European Digital Identity Wallets;

(b) lays down rules for trust services, in particular for electronic transactions;

(c) establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services, certificate services for website authentication, electronic archiving, electronic attestation of attributes, electronic signature creation devices, electronic seal creation devices, and electronic ledgers.

▼B

Article 2

Scope

▼M2

1. This Regulation applies to electronic identification schemes notified by a Member State, to European Digital Identity Wallets provided by a Member State and to trust service providers established in the Union.

▼B

2. This Regulation does not apply to the provision of trust services that are used exclusively within closed systems resulting from national law or from agreements between a defined set of participants.

▼M2

3. This Regulation does not affect Union or national law related to the conclusion and validity of contracts, other legal or procedural obligations relating to form, or sector-specific requirements relating to form.

▼M2

4. This Regulation is without prejudice to Regulation (EU) 2016/679 of the European Parliament and of the Council ([1]).

▼B

Article 3

Definitions

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

▼M2

(1) ‘electronic identification’ means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing another natural person or a legal person;

(2) ‘electronic identification means’ means a material and/or immaterial unit containing person identification data and which is used for authentication for an online service or, where appropriate, for an offline service;

(3) ‘person identification data’ means a set of data that is issued in accordance with Union or national law and that enables the establishment of the identity of a natural or legal person, or of a natural person representing another natural person or a legal person.

(4) ‘electronic identification scheme’ means a system for electronic identification under which electronic identification means are issued to natural or legal persons or natural persons representing other natural persons or legal persons;

(5) ‘authentication’ means an electronic process that enables the confirmation of the electronic identification of a natural or legal person or the confirmation of the origin and integrity of data in electronic form;

(5a) ‘user’ means a natural or legal person, or a natural person representing another natural person or a legal person, that uses trust services or electronic identification means provided in accordance with this Regulation;

(6) ‘relying party’ means a natural or legal person that relies upon electronic identification, European Digital Identity Wallets or other electronic identification means, or upon a trust service;

▼B

(7) ‘public sector body’ means a state, regional or local authority, a body governed by public law or an association formed by one or several such authorities or one or several such bodies governed by public law, or a private entity mandated by at least one of those authorities, bodies or associations to provide public services, when acting under such a mandate;

([1]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016on 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).

▼B

(8) ‘body governed by public law’ means a body defined in point (4) of Article 2(1) of Directive 2014/24/EU of the European Parliament and of the Council ([1]);

(9) ‘signatory’ means a natural person who creates an electronic signature;

(10) ‘electronic signature’ means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;

(11) ‘advanced electronic signature’ means an electronic signature which meets the requirements set out in Article 26;

(12) ‘qualified electronic signature’ means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures;

(13) ‘electronic signature creation data’ means unique data which is used by the signatory to create an electronic signature;

(14) ‘certificate for electronic signature’ means an electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person;

(15) ‘qualified certificate for electronic signature’ means a certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I;

▼M2

(16) ‘trust service’ means an electronic service normally provided for remuneration which consists of any of the following:

(a) the issuance of certificates for electronic signatures, certificates for electronic seals, certificates for website authentication or certificates for the provision of other trust services;

(b) the validation of certificates for electronic signatures, certificates for electronic seals, certificates for website authentication or certificates for the provision of other trust services;

(c) the creation of electronic signatures or electronic seals;

(d) the validation of electronic signatures or electronic seals;

(e) the preservation of electronic signatures, electronic seals, certificates for electronic signatures or certificates for electronic seals;

(f) the management of remote electronic signature creation devices or remote electronic seal creation devices;

(g) the issuance of electronic attestations of attributes;

(h) the validation of electronic attestation of attributes;

([1]) Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC (OJ L 94, 28.3.2014, p. 65).

▼M2

(i) the creation of electronic timestamps;

(j) the validation of electronic timestamps;

(k) the provision of electronic registered delivery services;

(l) the validation of data transmitted through electronic registered delivery services and related evidence;

(m) the electronic archiving of electronic data and electronic documents;

(n) the recording of electronic data in an electronic ledger;

▼B

(17) ‘qualified trust service’ means a trust service that meets the applicable requirements laid down in this Regulation;

▼M2

(18) ‘conformity assessment body’ means a conformity assessment body as defined in Article 2, point 13, of Regulation (EC) No 765/2008, which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides, or as competent to carry out certification of European Digital Identity Wallets or electronic identification means;

▼B

(19) ‘trust service provider’ means a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider;

(20) ‘qualified trust service provider’ means a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body;

▼M2

(21) ‘product’ means hardware or software, or relevant components of hardware or software, which are intended to be used for the provision of electronic identification and trust services;

▼B

(22) ‘electronic signature creation device’ means configured software or hardware used to create an electronic signature;

(23) ‘qualified electronic signature creation device’ means an electronic signature creation device that meets the requirements laid down in Annex II;

▼M2

(23a) ‘remote qualified electronic signature creation device’ means a qualified electronic signature creation device that is managed by a qualified trust service provider in accordance with Article 29a on behalf of a signatory;

▼M2

(23b) ‘remote qualified electronic seal creation device’ means a qualified electronic seal creation device that is managed by a qualified trust service provider in accordance with Article 39a on behalf of a seal creator;

▼B

(24) ‘creator of a seal’ means a legal person who creates an electronic seal;

(25) ‘electronic seal’ means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter’s origin and integrity;

(26) ‘advanced electronic seal’ means an electronic seal, which meets the requirements set out in Article 36;

(27) ‘qualified electronic seal’ means an advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal;

(28) ‘electronic seal creation data’ means unique data, which is used by the creator of the electronic seal to create an electronic seal;

(29) ‘certificate for electronic seal’ means an electronic attestation that links electronic seal validation data to a legal person and confirms the name of that person;

(30) ‘qualified certificate for electronic seal’ means a certificate for an electronic seal, that is issued by a qualified trust service provider and meets the requirements laid down in Annex III;

(31) ‘electronic seal creation device’ means configured software or hardware used to create an electronic seal;

(32) ‘qualified electronic seal creation device’ means an electronic seal creation device that meets mutatis mutandis the requirements laid down in Annex II;

(33) ‘electronic time stamp’ means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time;

(34) ‘qualified electronic time stamp’ means an electronic time stamp which meets the requirements laid down in Article 42;

(35) ‘electronic document’ means any content stored in electronic form, in particular text or sound, visual or audiovisual recording;

(36) ‘electronic registered delivery service’ means a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations;

▼B

(37) ‘qualified electronic registered delivery service’ means an electronic registered delivery service which meets the requirements laid down in Article 44;

▼M2

(38) ‘certificate for website authentication’ means an electronic attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued;

▼B

(39) ‘qualified certificate for website authentication’ means a certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV;

(40) ‘validation data’ means data that is used to validate an electronic signature or an electronic seal;

▼M2

(41) ‘validation’ means the process of verifying and confirming that data in electronic form are valid in accordance with this Regulation;

(42) ‘European Digital Identity Wallet’ means an electronic identification means which allows the user to securely store, manage and validate person identification data and electronic attestations of attributes for the purpose of providing them to relying parties and other users of European Digital Identity Wallets, and to sign by means of qualified electronic signatures or to seal by means of qualified electronic seals;

(43) ‘attribute’ means a characteristic, quality, right or permission of a natural or legal person or of an object;

(44) ‘electronic attestation of attributes’ means an attestation in electronic form that allows attributes to be authenticated;

(45) ‘qualified electronic attestation of attributes’ means an electronic attestation of attributes which is issued by a qualified trust service provider and meets the requirements laid down in Annex V;

(46) ‘electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source’ means an electronic attestation of attributes issued by a public sector body that is responsible for an authentic source or by a public sector body that is designated by the Member State to issue such attestations of attributes on behalf of the public sector bodies responsible for authentic sources in accordance with Article 45f and with Annex VII;

(47) ‘authentic source’ means a repository or system, held under the responsibility of a public sector body or private entity, that contains and provides attributes about a natural or legal person or object and that is considered to be a primary source of that information or recognised as authentic in accordance with Union or national law, including administrative practice;

▼M2

(48) ‘electronic archiving’ means a service ensuring the receipt, storage, retrieval and deletion of electronic data and electronic documents in order to ensure their durability and legibility as well as to preserve their integrity, confidentiality and proof of origin throughout the preservation period;

(49) ‘qualified electronic archiving service’ means an electronic archiving service which is provided by a qualified trust service provider and which meets the requirements laid down in Article 45j;

(50) ‘EU Digital Identity Wallet Trust Mark’ means a verifiable, simple and recognisable indication which is communicated in a clear manner that a European Digital Identity Wallet has been provided in accordance with this Regulation;

(51) ‘strong user authentication’ means an authentication based on the use of at least two authentication factors from different categories of either knowledge, something only the user knows, possession, something only the user possesses or inherence, something the user is, that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data;

(52) ‘electronic ledger’ means a sequence of electronic data records, ensuring the integrity of those records and the accuracy of the chronological ordering of those records;

(53) ‘qualified electronic ledger’ means an electronic ledger which is provided by a qualified trust service provider and which meets the requirements laid down in Article 45l;

(54) ‘personal data’ means any information as defined in Article 4, point (1), of Regulation (EU) 2016/679;

(55) ‘identity matching’ means a process where person identification data, or electronic identification means are matched with or linked to an existing account belonging to the same person;

(56) ‘data record’ means electronic data recorded with related metadata supporting the processing of the data;

(57) ‘offline mode’ means, as regards the use of European Digital Identity Wallets, an interaction between a user and a third party at a physical location using close proximity technologies, whereby the European Digital Identity Wallet is not required to access remote systems via electronic communication networks for the purpose of the interaction.

▼B

Article 4

Internal market principle

1. There shall be no restriction on the provision of trust services in the territory of a Member State by a trust service provider established in another Member State for reasons that fall within the fields covered by this Regulation.

▼B

2. Products and trust services that comply with this Regulation shall be permitted to circulate freely in the internal market.

▼M2

Article 5

Pseudonyms in electronic transaction

Without 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.

▼B

CHAPTER II

ELECTRONIC IDENTIFICATION

▼M2

SECTION 1

european digital identity wallet

Article 5a

European Digital Identity Wallets

1. For the purpose of ensuring that all natural and legal persons in the Union have secure, trusted and seamless cross-border access to public and private services, while having full control over their data, each Member State shall provide at least one European Digital Identity Wallet within 24 months of the date of entry into force of the implementing acts referred to in paragraph 23 of this Article and in Article 5c(6).

2. European Digital Identity Wallets shall be provided in one or more of the following ways:

(a) directly by a Member State;

(b) under a mandate from a Member State;

(c) independently of a Member State but recognised by that Member State.

3. The source code of the application software components of European Digital Identity Wallets shall be open-source licensed. Member States may provide that, for duly justified reasons, the source code of specific components other than those installed on user devices shall not be disclosed.

4. European Digital Identity Wallets shall enable the user, in a manner that is user-friendly, transparent, and traceable by the user, to:

(a) securely request, obtain, select, combine, store, delete, share and present, under the sole control of the user, person identification data and, where applicable, in combination with electronic attestations of attributes, to authenticate to relying parties online and, where appropriate, in offline mode, in order to access public and private services, while ensuring that selective disclosure of data is possible;

▼M2

(b) generate pseudonyms and store them encrypted and locally within the European Digital Identity Wallet;

(c) securely authenticate another person's European Digital Identity Wallet, and receive and share person identification data and electronic attestations of attributes in a secured way between the two European Digital Identity Wallets;

(d) access a log of all transactions carried out through the European Digital Identity Wallet via a common dashboard enabling the user to:

(i) view an up-to-date list of relying parties with which the user has established a connection and, where applicable, all data exchanged;

(ii) easily request the erasure by a relying party of personal data pursuant to Article 17 of the Regulation (EU) 2016/679;

(iii) easily report a relying party to the competent national data protection authority, where an allegedly unlawful or suspicious request for data is received;

(e) sign by means of qualified electronic signatures or seal by means of qualified electronic seals;

(f) download, to the extent technically feasible, the user's data, electronic attestation of attributes and configurations;

(g) exercise the user's rights to data portability.

5. European Digital Identity Wallets shall, in particular:

(a) support common protocols and interfaces:

(i) for issuance of person identification data, qualified and non-qualified electronic attestations of attributes or qualified and non-qualified certificates to the European Digital Identity Wallet;

(ii) for relying parties to request and validate person identification data and electronic attestations of attributes;

(iii) for the sharing and presentation to relying parties of person identification data, electronic attestation of attributes or of selectively disclosed related data online and, where appropriate, in offline mode;

(iv) for the user to allow interaction with the European Digital Identity Wallet and display an EU Digital Identity Wallet Trust Mark;

(v) to securely onboard the user by using an electronic identification means in accordance with Article 5a(24);

(vi) for interaction between two persons' European Digital Identity Wallets for the purpose of receiving, validating and sharing person identification data and electronic attestations of attributes in a secure manner;

▼M2

(vii) for authenticating and identifying relying parties by implementing authentication mechanisms in accordance with Article 5b;

(viii) for relying parties to verify the authenticity and validity of European Digital Identity Wallets;

(ix) for requesting a relying party the erasure of personal data pursuant to Article 17 of Regulation (EU) 2016/679;

(x) for reporting a relying party to the competent national data protection authority where an allegedly unlawful or suspicious request for data is received;

(xi) for the creation of qualified electronic signatures or electronic seals by means of qualified electronic signature or electronic seal creation devices;

(b) not provide any information to trust service providers of electronic attestations of attributes about the use of those electronic attestations;

(c) ensure that the relying parties can be authenticated and identified by implementing authentication mechanisms in accordance with Article 5b;

(d) meet the requirements set out in Article 8 with regard to assurance level high, in particular as applied to the requirements for identity proofing and verification, and electronic identification means management and authentication;

(e) in the case of the electronic attestation of attributes with embedded disclosure policies, implement the appropriate mechanism to inform the user that the relying party or the user of the European Digital Identity Wallet requesting that electronic attestation of attributes has the permission to access such attestation;

(f) ensure that the person identification data, which is available from the electronic identification scheme under which the European Digital Identity Wallet is provided, uniquely represents the natural person, legal person or the natural person representing the natural or legal person, and is associated with that European Digital Identity Wallet;

(g) offer all natural persons the ability to sign by means of qualified electronic signatures by default and free of charge.

Notwithstanding point (g) of the first subparagraph, Member States may provide for proportionate measures to ensure that the use of qualified electronic signatures free-of-charge by natural persons is limited to non-professional purposes.

6. Member State shall inform users, without delay, of any security breach that could have entirely or partially compromised their European Digital Identity Wallet or its contents, in particular if their European Digital Identity Wallet has been suspended or revoked pursuant to Article 5e.

▼M2

7. Without prejudice to Article 5f, Member States may provide, in accordance with national law, for additional functionalities of European Digital Identity Wallets, including interoperability with existing national electronic identification means. Those additional functionalities shall comply with this Article.

8. Member States shall provide validation mechanisms free-of-charge, in order to:

(a) ensure that the authenticity and validity of European Digital Identity Wallets can be verified;

(b) allow users to verify the authenticity and validity of the identity of relying parties registered in accordance with Article 5b.

9. Member States shall ensure that the validity of the European Digital Identity Wallet can be revoked in the following circumstances:

(a) upon the explicit request of the user;

(b) where the security of the European Digital Identity Wallet has been compromised;

(c) upon the death of the user or cease of activity of the legal person.

10. Providers of European Digital Identity Wallets shall ensure that users can easily request technical support and report technical problems or any other incidents having a negative impact on the use of European Digital Identity Wallets.

11. European Digital Identity Wallets shall be provided under an electronic identification scheme with assurance level high.

12. European Digital Identity Wallets shall ensure security-by-design.

13. The issuance, use and revocation of the European Digital Identity Wallets shall be free of charge to all natural persons.

14. Users shall have full control of the use of and of the data in their European Digital Identity Wallet. The provider of the European Digital Identity Wallet shall neither collect information about the use of the European Digital Identity Wallet which is not necessary for the provision of European Digital Identity Wallet services, nor combine person identification data or any other personal data stored or relating to the use of the European Digital Identity 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 European Digital Identity Wallet services, unless the user has expressly requested otherwise. Personal data relating to the provision of the European Digital Identity Wallet shall be kept logically separate from any other data held by the provider of the European Digital Identity Wallet. If the European Digital Identity Wallet is provided by private parties in accordance with paragraph 2, points (b) and (c), of this Article, the provisions of Article 45h(3) shall apply *mutatis mutandis*.

▼M2

15. The use of European Digital Identity Wallets shall be voluntary. Access to public and private services, access to the labour market and freedom to conduct business shall not in any way be restricted or made disadvantageous to natural or legal persons that do not use European Digital Identity Wallets. It shall remain possible to access public and private services by other existing identification and authentication means.

16. The technical framework of the European Digital Identity Wallet shall:

(a) 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;

(b) enable privacy preserving techniques which ensure unlikeability, where the attestation of attributes does not require the identification of the user.

17. Any processing of personal data carried out by the Member States or on their behalf by bodies or parties responsible for the provision of European Digital Identity Wallets as electronic identification means shall be carried out in accordance with appropriate and effective data protection measures. Compliance of such processing with Regulation (EU) 2016/679 shall be demonstrated. Member States may introduce national provisions to further specify the application of such measures.

18. Member States shall, without undue delay, notify the Commission of information about:

(a) the body responsible for establishing and maintaining the list of registered relying parties that rely on European Digital Identity Wallets in accordance with Article 5b(5) and the location of that list;

(b) the bodies responsible for the provision of European Digital Identity Wallets in accordance with Article 5a(1);

(c) the bodies responsible for ensuring that the person identification data is associated with the European Digital Identity Wallet in accordance with Article 5a(5), point (f);

(d) the mechanism allowing for the validation of the person identification data referred to in Article 5a(5), point (f), and of the identity of the relying parties;

(e) the mechanism by which to validate the authenticity and validity of European Digital Identity Wallets.

The Commission shall make available the information notified pursuant to the first subparagraph to the public through a secure channel, in electronically signed or sealed form suitable for automated processing.

▼M2

19. Without prejudice to paragraph 22 of this Article, Article 11 shall apply *mutatis mutandis* to the European Digital Identity Wallet.

20. Article 24(2), points (b), and (d) to (h), shall apply *mutatis mutandis* to providers of European Digital Identity Wallets.

21. European Digital Identity Wallets shall be made accessible for use, by persons with disabilities, on an equal basis with other users, in accordance with Directive (EU) 2019/882 of the European Parliament and of the Council ([1]).

22. For the purposes of the provision of European Digital Identity Wallets, European Digital Identity Wallets and the electronic identification schemes under which they are provided shall not be subject to the requirements laid down in Articles 7, 9, 10, 12 and 12a.

23. By 21 November 2024, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the requirements referred to in paragraphs 4, 5, 8 and 18 of this Article on the implementation of the European Digital Identity Wallet. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

24. The Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures in order to facilitate the onboarding of users to the European Digital Identity Wallet either by electronic identification means conforming to assurance level high or by electronic identification means conforming to assurance level substantial in conjunction with additional remote onboarding procedures that together meet the requirements of assurance level high. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 5b

European Digital Identity Wallet-Relying Parties

1. Where a relying party intends to rely upon European Digital Identity Wallets for the provision of public or private services by means of digital interaction, the relying party shall register in the Member State where it is established.

2. The registration process shall be cost-effective and proportionate-to-risk. The relying party shall provide at least:

(a) the information necessary to authenticate to European Digital Identity Wallets, which as a minimum includes:

(i) the Member State in which the relying party is established; and

([1]) Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019on the accessibility requirements for products and services (OJ L 151, 7.6.2019, p. 70).

▼M2

(ii) the name of the relying party and, where applicable, its registration number as stated in an official record together with identification data of that official record;

(b) the contact details of the relying party;

(c) the intended use of European Digital Identity Wallets, including an indication of the data to be requested by the relying party from users.

3. Relying parties shall not request users to provide any data other than that indicated pursuant to paragraph 2, point (c).

4. Paragraphs 1 and 2 shall be without prejudice to Union or national law that is applicable to the provision of specific services.

5. Member States shall make the information referred to in paragraph 2 publicly available online in electronically signed or sealed form suitable for automated processing.

6. Relying parties registered in accordance with this Article shall inform Member States without delay about any changes to the information provided in the registration pursuant to paragraph 2.

7. Member States shall provide a common mechanism for allowing the identification and authentication of relying parties, as referred to in Article 5a(5), point (c).

8. Where relying parties intend to rely upon European Digital Identity Wallets, they shall identify themselves to the user.

9. Relying parties shall be responsible for carrying out the procedure for authenticating and validating person identification data and electronic attestation of attributes requested from European Digital Identity Wallets. Relying parties shall not refuse the use of pseudonyms, where the identification of the user is not required by Union or national law.

10. Intermediaries acting on behalf of relying parties shall be deemed to be relying parties and shall not store data about the content of the transaction.

11. By 21 November 2024, the Commission shall establish technical specifications and procedures for the requirements referred to in paragraphs 2, 5 and 6 to 9 of this Article by means of implementing acts on the implementation of European Digital Identity Wallets as referred to in Article 5a(23). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 5c

Certification of European Digital Identity Wallets

1. The conformity of European Digital Identity Wallets and the electronic identification scheme under which they are provided with the requirements laid down in Article 5a(4), (5), (8), the requirement for logical separation laid down in Article 5a(14) and, where applicable, with the standards and technical specifications referred to in Article 5a (24), shall be certified by conformity assessment bodies designated by Member States.

▼M2

2. Certification of the conformity of European Digital Identity Wallets with requirements referred to in paragraph 1 of this Article, or parts thereof, that are relevant for cybersecurity shall be carried out in accordance with European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 of the European Parliament and of the Council ([1]) and referred to in the implementing acts referred to in paragraph 6 of this Article.

3. For requirements referred to in paragraph 1 of this Article that are not relevant for cybersecurity, and, for requirements referred to in paragraph 1 of this Article that are relevant for cybersecurity, to the extent that cybersecurity certification schemes as referred to in paragraph 2 of this Article do not, or only partially, cover those cybersecurity requirements, also for those requirements, Member States shall establish national certification schemes following the requirements set out in the implementing acts referred to in paragraph 6 of this Article. Member States shall transmit their draft national certification schemes to the European Digital Identity Cooperation Group established pursuant to Article 46e(1) (the 'Cooperation Group'). The Cooperation Group may issue opinions and recommendations.

4. Certification pursuant to paragraph 1 shall be valid for up to five years, provided that a vulnerability assessment is carried out every two years. Where a vulnerability is identified and not remedied in a timely manner, certification shall be cancelled.

5. 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.

6. By 21 November 2024, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the certification of European Digital Identity Wallets referred to in paragraph 1, 2 and 3 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

7. Member States shall communicate to the Commission the names and addresses of the conformity assessment bodies referred to in paragraph 1. The Commission shall make that information available to all Member States.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 47 establishing specific criteria to be met by the designated conformity assessment bodies referred to in paragraph 1 of this Article.

([1]) Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).

▼M2

Article 5d

Publication of a list of certified European Digital Identity Wallets

1. Member States shall inform the Commission and the Cooperation Group established pursuant to Article 46e(1) without undue delay of European Digital Identity Wallets that have been provided pursuant to Article 5a and certified by the conformity assessment bodies referred to in Article 5c(1). They shall inform the Commission and the Cooperation Group established pursuant to Article 46e(1), without undue delay if a certification is cancelled and shall state the reasons for the cancellation.

2. Without prejudice to Article 5a(18), the information provided by Member States referred to in paragraph 1 of this Article shall include at least:

(a) the certificate and certification assessment report of the certified European Digital Identity Wallet;

(b) a description of the electronic identification scheme under which the European Digital Identity Wallet is provided;

(c) the applicable supervisory regime and information on the liability regime with respect to the party providing the European Digital Identity Wallet;

(d) the authority or authorities responsible for the electronic identification scheme;

(e) arrangements for suspension or revocation of the electronic identification scheme or authentication or of the compromised parts concerned.

3. On the basis of the information received pursuant to paragraph 1, the Commission shall establish, publish in the *Official Journal of the European Union* and maintain in a machine-readable form a list of certified European Digital Identity Wallets.

4. A Member State may submit a request to the Commission to remove a European Digital Identity Wallet and the electronic identification scheme under which it is provided from the list referred to in paragraph 3.

5. Where there are changes to the information provided pursuant to paragraph 1, the Member State shall provide the Commission with updated information.

6. The Commission shall keep the list referred to in paragraph 3 updated by publishing in the *Official Journal of the European Union* the corresponding amendments to the list within one month of receipt of a request pursuant to paragraph 4 or of updated information pursuant to paragraph 5.

7. By 21 November 2024, the Commission shall establish the formats and procedures applicable for the purposes of paragraphs 1, 4 and 5 of this Article by means of implementing acts on the implementation of European Digital Identity Wallets as referred to in Article 5a(23). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

▼M2

Article 5e

Security breach of European Digital Identity Wallets

1. Where European Digital Identity Wallets provided pursuant to Article 5a, the validation mechanisms referred to in Article 5a(8) or the electronic identification scheme under which the European Digital Identity Wallets are provided are breached or partly compromised in a manner that affects their reliability or the reliability of other European Digital Identity Wallets, the Member State that provided the European Digital Identity Wallets shall, without undue delay, suspend the provision and the use of European Digital Identity Wallets.

Where justified by the severity of the security breach or compromise referred to in the first subparagraph, the Member State shall withdraw European Digital Identity Wallets without undue delay.

The Member State shall inform the users affected, the single points of contact designated pursuant to Article 46c(1), the relying parties and the Commission accordingly.

2. If the security breach or compromise referred to in paragraph 1, first subparagraph, of this Article is not remedied within three months of the suspension, the Member State that provided the European Digital Identity Wallets shall withdraw European Digital Identity Wallets and revoke their validity. The Member State shall inform the users affected, the single points of contact designated pursuant to Article 46c(1), the relying parties and the Commission of the withdrawal accordingly.

3. Where the security breach or compromise referred to in paragraph 1, first subparagraph, of this Article is remedied, the providing Member State shall re-establish the provision and the use of European Digital Identity Wallets and inform the affected users and relying parties, the single points of contact designated pursuant to Article 46c(1) and the Commission without undue delay.

4. The Commission shall publish in the *Official Journal of the European Union* the corresponding amendments to the list referred to in Article 5d without undue delay.

5. By 21 November 2024, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the measures referred to in paragraphs 1, 2 and 3 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 5f

Cross-border reliance on European Digital Identity Wallets

1. Where Member States require electronic identification and authentication to access an online service provided by a public sector body, they shall also accept European Digital Identity Wallets that are provided in accordance with this Regulation.

▼M2

2. Where private relying parties that provide services, with the exception of microenterprises and small enterprises as defined in Article 2 of the Annex to Commission Recommendation 2003/361/EC ([1]), are required by Union or national law to use strong user authentication for online identification or where strong user authentication for online identification is required by contractual obligation, including in the areas of transport, energy, banking, financial services, social security, health, drinking water, postal services, digital infrastructure, education or telecommunications, those private relying parties shall, no later than 36 months from the date of entry into force of the implementing acts referred to in Article 5a(23) and Article 5c(6) and only upon the voluntary request of the user, also accept European Digital Identity Wallets that are provided in accordance with this Regulation.

3. Where providers of very large online platforms as referred to in Article 33 of Regulation (EU) 2022/2065 of the European Parliament and of the Council ([2]) require user authentication for access to online services, they shall also accept and facilitate the use of European Digital Identity Wallets that are provided in accordance with this Regulation for user authentication only upon the voluntary request of the user and in respect of the minimum data necessary for the specific online service for which authentication is requested.

4. In cooperation with Member States, the Commission shall facilitate the development of codes of conduct in close collaboration with all relevant stakeholders, including civil society, in order to contribute to the wide availability and usability of European Digital Identity Wallets within the scope of this Regulation, and to encourage service providers to complete the development of codes of conduct.

5. Within 24 months after deployment of the European Digital Identity Wallets, the Commission shall assess the demand for, and the availability and usability of, European Digital Identity Wallets, taking into account criteria such as user take-up, cross-border presence of service providers, technological developments, evolution in usage patterns and consumer demand.

▼M2

SECTION 2

electronic identification schemes

▼B

Article 6

Mutual recognition

1. When an electronic identification using an electronic identification means and authentication is required under national law or by administrative practice to access a service provided by a public sector

([1]) Commission Recommendation 2003/361/EC of 6 May 2003concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

([2]) Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (OJ L 277, 27.10.2022, p. 1).

▼B

body online in one Member State, the electronic identification means issued in another Member State shall be recognised in the first Member State for the purposes of cross-border authentication for that service online, provided that the following conditions are met:

(a) the electronic identification means is issued under an electronic identification scheme that is included in the list published by the Commission pursuant to Article 9;

(b) the assurance level of the electronic identification means corresponds to an assurance level equal to or higher than the assurance level required by the relevant public sector body to access that service online in the first Member State, provided that the assurance level of that electronic identification means corresponds to the assurance level substantial or high;

(c) the relevant public sector body uses the assurance level substantial or high in relation to accessing that service online.

Such recognition shall take place no later than 12 months after the Commission publishes the list referred to in point (a) of the first subparagraph.

2. An electronic identification means which is issued under an electronic identification scheme included in the list published by the Commission pursuant to Article 9 and which corresponds to the assurance level low may be recognised by public sector bodies for the purposes of cross-border authentication for the service provided online by those bodies.

Article 7

Eligibility for notification of electronic identification schemes

An electronic identification scheme shall be eligible for notification pursuant to Article 9(1) provided that all of the following conditions are met:

(a) the electronic identification means under the electronic identification scheme are issued:

(i) by the notifying Member State;

(ii) under a mandate from the notifying Member State; or

(iii) independently of the notifying Member State and are recognised by that Member State;

(b) the electronic identification means under the electronic identification scheme can be used to access at least one service which is provided by a public sector body and which requires electronic identification in the notifying Member State;

(c) the electronic identification scheme and the electronic identification means issued thereunder meet the requirements of at least one of the assurance levels set out in the implementing act referred to in Article 8(3);

▼B

(d) the notifying Member State ensures that the person identification data uniquely representing the person in question is attributed, in accordance with the technical specifications, standards and procedures for the relevant assurance level set out in the implementing act referred to in Article 8(3), to the natural or legal person referred to in point 1 of Article 3 at the time the electronic identification means under that scheme is issued;

(e) the party issuing the electronic identification means under that scheme ensures that the electronic identification means is attributed to the person referred to in point (d) of this Article in accordance with the technical specifications, standards and procedures for the relevant assurance level set out in the implementing act referred to in Article 8(3);

(f) the notifying Member State ensures the availability of authentication online, so that any relying party established in the territory of another Member State is able to confirm the person identification data received in electronic form.

For relying parties other than public sector bodies the notifying Member State may define terms of access to that authentication. The cross-border authentication shall be provided free of charge when it is carried out in relation to a service online provided by a public sector body.

Member States shall not impose any specific disproportionate technical requirements on relying parties intending to carry out such authentication, where such requirements prevent or significantly impede the interoperability of the notified electronic identification schemes;

▼M2

(g) at least six months prior to notification pursuant to Article 9(1), the notifying Member State provides the other Member States, for the purposes of Article 12(5), with a description of that scheme in accordance with the procedural arrangements established by the implementing acts adopted pursuant to Article 12(6);

▼B

(h) the electronic identification scheme meets the requirements set out in the implementing act referred to in Article 12(8).

Article 8

Assurance levels of electronic identification schemes

1. An electronic identification scheme notified pursuant to Article 9 (1) shall specify assurance levels low, substantial and/or high for electronic identification means issued under that scheme.

2. The assurance levels low, substantial and high shall meet respectively the following criteria:

▼B

(a) assurance level low shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a limited degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of misuse or alteration of the identity;

(b) assurance level substantial shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a substantial degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease substantially the risk of misuse or alteration of the identity;

(c) assurance level high shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a higher degree of confidence in the claimed or asserted identity of a person than electronic identification means with the assurance level substantial, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to prevent misuse or alteration of the identity.

▼M2

3. By 18 September 2015, taking into account relevant international standards and subject to paragraph 2, the Commission shall, by means of implementing acts, set out minimum technical specifications, standards and procedures with reference to which assurance levels low, substantial and high are specified for electronic identification means.

▼B

Those minimum technical specifications, standards and procedures shall be set out by reference to the reliability and quality of the following elements:

(a) the procedure to prove and verify the identity of natural or legal persons applying for the issuance of electronic identification means;

(b) the procedure for the issuance of the requested electronic identification means;

(c) the authentication mechanism, through which the natural or legal person uses the electronic identification means to confirm its identity to a relying party;

(d) the entity issuing the electronic identification means;

(e) any other body involved in the application for the issuance of the electronic identification means; and

(f) the technical and security specifications of the issued electronic identification means.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

▼B

Article 9

Notification

1. The notifying Member State shall notify to the Commission the following information and, without undue delay, any subsequent changes thereto:

(a) a description of the electronic identification scheme, including its assurance levels and the issuer or issuers of electronic identification means under the scheme;

(b) the applicable supervisory regime and information on the liability regime with respect to the following:

(i) the party issuing the electronic identification means; and

(ii) the party operating the authentication procedure;

(c) the authority or authorities responsible for the electronic identification scheme;

(d) information on the entity or entities which manage the registration of the unique person identification data;

(e) a description of how the requirements set out in the implementing acts referred to in Article 12(8) are met;

(f) a description of the authentication referred to in point (f) of Article 7;

(g) arrangements for suspension or revocation of either the notified electronic identification scheme or authentication or the compromised parts concerned.

▼M2

2. The Commission shall, without undue delay, publish in the *Official Journal of the European Union* a list of the electronic identification schemes which were notified pursuant to paragraph 1 together with basic information about those schemes.

3. The Commission shall publish in the *Official Journal of the European Union* the amendments to the list referred to in paragraph 2 within one month of the date of receipt of that notification.

▼B

4. A Member State may submit to the Commission a request to remove an electronic identification scheme notified by that Member State from the list referred to in paragraph 2. The Commission shall publish in the *Official Journal of the European Union* the corresponding amendments to the list within one month from the date of receipt of the Member State's request.

▼B

5. The Commission may, by means of implementing acts, define the circumstances, formats and procedures of notifications under paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 10

▼M2

Security breach of electronic identification schemes

▼B

1. Where either the electronic identification scheme notified pursuant to Article 9(1) or the authentication referred to in point (f) of Article 7 is breached or partly compromised in a manner that affects the reliability of the cross-border authentication of that scheme, the notifying Member State shall, without delay, suspend or revoke that cross-border authentication or the compromised parts concerned, and shall inform other Member States and the Commission.

2. When the breach or compromise referred to in paragraph 1 is remedied, the notifying Member State shall re-establish the cross-border authentication and shall inform other Member States and the Commission without undue delay.

3. If the breach or compromise referred to in paragraph 1 is not remedied within three months of the suspension or revocation, the notifying Member State shall notify other Member States and the Commission of the withdrawal of the electronic identification scheme.

The Commission shall publish in the *Official Journal of the European Union* the corresponding amendments to the list referred to in Article 9 (2) without undue delay.

Article 11

Liability

1. The notifying Member State shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with its obligations under points (d) and (f) of Article 7 in a cross-border transaction.

2. The party issuing the electronic identification means shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligation referred to in point (e) of Article 7 in a cross-border transaction.

3. The party operating the authentication procedure shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to ensure the correct operation of the authentication referred to in point (f) of Article 7 in a cross-border transaction.

4. Paragraphs 1, 2 and 3 shall be applied in accordance with national rules on liability.

▼B

5. Paragraphs 1, 2 and 3 are without prejudice to the liability under national law of parties to a transaction in which electronic identification means falling under the electronic identification scheme notified pursuant to Article 9(1) are used.

▼M2

Article 11a

Cross-border identity matching

1. When acting as relying parties for cross-border services, Member States shall ensure unequivocal identity matching for natural persons using notified electronic identification means or European Digital Identity Wallets.

2. Member States shall provide for technical and organisational measures to ensure a high level of protection of personal data used for identity matching and to prevent the profiling of users.

3. By 21 November 2024, the Commission shall establish a list of reference standards and, where necessary, establish specifications and procedures for the requirements referred to in paragraph 1 of this Article by means of implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

▼B

Article 12

▼M2

Interoperability

▼B

1. The national electronic identification schemes notified pursuant to Article 9(1) shall be interoperable.

2. For the purposes of paragraph 1, an interoperability framework shall be established.

3. The interoperability framework shall meet the following criteria:

(a) it aims to be technology neutral and does not discriminate between any specific national technical solutions for electronic identification within a Member State;

(b) it follows European and international standards, where possible;

▼M2

(c) it facilitates the implementation of privacy and security by design.

▼B

4. The interoperability framework shall consist of:

(a) a reference to minimum technical requirements related to the assurance levels under Article 8;

▼B

(b) a mapping of national assurance levels of notified electronic identification schemes to the assurance levels under Article 8;

(c) a reference to minimum technical requirements for interoperability;

▼M2

(d) a reference to a minimum set of person identification data necessary to uniquely represent a natural or legal person, or a natural person representing another natural person or a legal person, which is available from electronic identification schemes;

▼B

(e) rules of procedure;

(f) arrangements for dispute resolution; and

(g) common operational security standards.

▼M2

5. Member States shall carry out peer reviews of the electronic identification schemes that fall within the scope of this Regulation and that are to be notified pursuant to Article 9(1), point (a).

6. By 18 March 2025, the Commission shall, by means of implementing acts, establish the necessary procedural arrangements for the peer reviews referred to in paragraph 5 of this Article with a view to fostering a high level of trust and security appropriate to the degree of risk. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

———————

8. By 18 September 2025, for the purpose of setting uniform conditions for the implementation of the requirement under paragraph 1 of this Article, the Commission shall, subject to the criteria set out in paragraph 3 of this Article and taking into account the results of the cooperation between Member States, adopt implementing acts on the interoperability framework as set out in paragraph 4 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

▼B

9. The implementing acts referred to in paragraphs 7 and 8 of this Article shall be adopted in accordance with the examination procedure referred to in Article 48(2).

▼M2

Article 12a

Certification of electronic identification schemes

1. The conformity of electronic identification schemes to be notified with the cybersecurity requirements laid down in this Regulation, including conformity with the cybersecurity relevant requirements set out in Article 8(2) regarding the assurance levels of electronic identification schemes, shall be certified by conformity assessment bodies designated by Member States.

▼M2

2. Certification pursuant to paragraph 1 of this Article shall be carried out under a relevant cybersecurity certification scheme pursuant to Regulation (EU) 2019/881 or parts thereof, insofar as the cybersecurity certificate or parts thereof cover those cybersecurity requirements.

3. Certification pursuant to paragraph 1 shall be valid for up to five years, provided that a vulnerability assessment is carried out every two years. Where a vulnerability is identified and not remedied within three months of such identification, certification shall be cancelled.

4. Notwithstanding paragraph 2, Member States may request, in accordance with that paragraph, additional information from a notifying Member State about electronic identification schemes or part thereof certified.

5. The peer review of electronic identification schemes referred to in Article 12(5) shall not apply to electronic identification schemes or parts of such schemes certified in accordance with paragraph 1 of this Article. Member States may use a certificate or a statement of conformity, issued in accordance with a relevant certification scheme or parts of such schemes, with the non-cybersecurity-related requirements set out in Article 8(2) regarding the assurance level of electronic identification schemes.

6. Member States shall communicate to the Commission the names and addresses of the conformity assessment bodies referred to in paragraph 1. The Commission shall make that information available to all Member States.

Article 12b

Access to hardware and software features

Where providers of European Digital Identity Wallets and issuers of notified electronic identification means that act in a commercial or professional capacity and use core platform services as defined in Article 2, point (2), of Regulation (EU) 2022/1925 of the European Parliament and of the Council ([1]) for the purpose or in the course of providing European Digital Identity Wallet services and electronic identification means to end-users are business users as defined in Article 2, point (21), of that Regulation, gatekeepers shall in particular allow them effective interoperability with, and, for the purposes of interoperability, access to, the same operating system, hardware or software features. Such effective interoperability and access shall be allowed free of charge and regardless of whether the hardware or software features are part of the operating system, are available to, or are used by, that gatekeeper when providing such services, within the meaning of Article 6(7) of Regulation (EU) 2022/1925. This Article is without prejudice to Article 5a(14) of this Regulation.

([1]) Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (OJ L 265, 12.10.2022, p. 1).

▼B

CHAPTER III

TRUST SERVICES

SECTION 1

General provisions

Article 13

Liability and burden of proof

▼M2

1. Notwithstanding paragraph 2 of this Article and without prejudice to Regulation (EU) 2016/679, trust service providers shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under this Regulation. Any natural or legal person who has suffered material or non-material damage as a result of an infringement of this Regulation by a trust service provider shall have the right to seek compensation in accordance with Union and national law.

The burden of proving the intention or negligence of a non-qualified trust service provider shall lie with the natural or legal person claiming the damage referred to in the first subparagraph.

The intention or negligence of a qualified trust service provider shall be presumed unless that qualified trust service provider proves that the damage referred to in the first subparagraph occurred without the intention or negligence of that qualified trust service provider.

▼B

2. Where trust service providers duly inform their customers in advance of the limitations on the use of the services they provide and where those limitations are recognisable to third parties, trust service providers shall not be liable for damages arising from the use of services exceeding the indicated limitations.

3. Paragraphs 1 and 2 shall be applied in accordance with national rules on liability.

▼M2

Article 14

International aspects

1. Trust services provided by trust service providers established in a third country or by an international organisation shall be recognised as legally equivalent to qualified trust services provided by qualified trust service providers established in the Union, where the trust services originating from the third country or from the international organisation are recognised by means of implementing acts or an agreement concluded between the Union and the third country or the international organisation pursuant to Article 218 TFEU.

The implementing acts referred to in the first subparagraph shall be adopted in accordance with the examination procedure referred to in Article 48(2).

▼M2

2. The implementing acts and the agreement referred to in paragraph 1 shall ensure that the requirements applicable to qualified trust service providers established in the Union and the qualified trust services they provide are met by the trust service providers in the third country concerned or by the international organisation and by the trust services they provide. Third countries and international organisations shall in particular establish, maintain and publish a trusted list of recognised trust service providers.

3. The agreement referred to in paragraph 1 shall ensure that the qualified trust services provided by qualified trust service providers established in the Union are recognised as legally equivalent to trust services provided by trust service providers in the third country or by the international organisation with which the agreement is concluded.

Article 15

Accessibility for persons with disabilities and special needs

The provision of electronic identification means, trust services and end-user products that are used in the provision of those services shall be made available in plain and intelligible language, in accordance with the United Nations Convention on the Rights of Persons with Disabilities and with the accessibility requirements of Directive (EU) 2019/882, thus also benefiting persons who experience functional limitations, such as elderly people, and persons with limited access to digital technologies.

Article 16

Penalties

1. Without prejudice to Article 31 of Directive (EU) 2022/2555 of the European Parliament and of the Council ([1]), Member States shall lay down the rules on penalties applicable to infringements of this Regulation. Those penalties shall be effective, proportionate and dissuasive.

2. Member States shall ensure that infringements of this Regulation by qualified and non-qualified trust service providers be subject to administrative fines of a maximum of at least:

(a) EUR 5 000 000 where the trust service provider is a natural person; or

(b) where the trust service provider is a legal person, EUR 5 000 000 or 1 % of the total worldwide annual turnover of the undertaking to which the trust service provider belonged in the financial year preceding the year in which the infringement occurred, whichever is higher.

([1]) Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80).

▼M2

3. Depending on the legal system of the Member States, the rules on administrative fines may be applied in such a manner that the fine is initiated by the competent supervisory body and imposed by competent national courts. The application of such rules in those Member States shall ensure that those legal remedies are effective and have an equivalent effect to administrative fines imposed directly by supervisory authorities.

▼B

SECTION 2

▼M2

Non-qualified trust services

_____

▼M1

_____

▼M2

Article 19a

Requirements for non-qualified trust service providers

1. A non-qualified trust service provider providing non-qualified trust services shall:

(a) have appropriate policies and take corresponding measures to manage legal, business, operational and other direct or indirect risks to the provision of the non-qualified trust service, which shall, notwithstanding Article 21 of Directive (EU) 2022/2555, include at least measures relating to:

(i) registration and onboarding procedures for a trust service;

(ii) procedural or administrative checks needed to provide trust services;

(iii) the management and implementation of trust services;

(b) notifying the supervisory body, the identifiable affected individuals, the public if it is of public interest and, where applicable, other relevant competent authorities, of any security breaches or disruptions in the provision of the service or the implementation of the measures referred to in point (a) (i), (ii) or (iii), that have a significant impact on the trust service provided or on the personal data maintained therein, without undue delay and in any case no later than 24 hours of having become aware of any security breaches or disruptions.

2. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for paragraph 1, point (a), of this Article. Compliance with the requirements laid down in this Article shall be presumed where those standards, specifications and procedures are met. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

▼B

SECTION 3

Qualified trust services

Article 20

Supervision of qualified trust service providers

▼M2

1. Qualified trust service providers shall be audited at their own expense at least every 24 months by a conformity assessment body. The audit shall confirm that the qualified trust service providers and the qualified trust services provided by them fulfil the requirements laid down in this Regulation and in Article 21 of Directive (EU) 2022/2555. Qualified trust service providers shall submit the resulting conformity assessment report to the supervisory body within three working days of receipt.

1a. Qualified trust service providers shall inform the supervisory body at the latest one month before any planned audits and shall allow the supervisory body to participate as an observer upon request.

1b. Member States shall, without undue delay, notify to the Commission the names, addresses and accreditation details of the conformity assessment bodies referred to in paragraph 1 and any subsequent changes thereto. The Commission shall make that information available to all Member States.

2. Without prejudice to paragraph 1, the supervisory body may at any time audit or request a conformity assessment body to perform a conformity assessment of the qualified trust service providers, at the expense of those trust service providers, to confirm that they and the qualified trust services provided by them fulfil the requirements laid down in this Regulation. Where personal data protection rules appear to have been breached, the supervisory body shall, without undue delay, inform the competent supervisory authorities established pursuant to Article 51 of Regulation (EU) 2016/679.

3. Where the qualified trust service provider fails to fulfil any of the requirements set out by this Regulation, the supervisory body shall require it to provide a remedy within a set time limit, if applicable.

Where that provider does not provide a remedy and, where applicable within the time limit set by the supervisory body, the supervisory body, where justified in particular by the extent, duration and consequences of that failure, shall withdraw the qualified status of that provider or of the affected service it provides.

3a. Where the competent authorities designated or established pursuant to Article 8(1) of Directive (EU) 2022/2555 informs the supervisory body that the qualified trust service provider fails to fulfil any of the requirements set out in Article 21 of that Directive, the supervisory body, where justified in particular by the extent, duration and consequences of that failure, shall withdraw the qualified status of that provider or of the affected service that it provides.

▼M2

3b. Where the supervisory authorities established pursuant to Article 51 of Regulation (EU) 2016/679 informs the supervisory body that the qualified trust service provider fails to fulfil any of the requirements set out in that Regulation, the supervisory body, where justified in particular by the extent, duration and consequences of that failure, shall withdraw the qualified status of that provider or of the affected service it provides.

3c. The supervisory body shall inform the qualified trust service provider of the withdrawal of its qualified status or of the qualified status of the service concerned. The supervisory body shall inform the body notified pursuant to Article 22(3) of this Regulation for the purposes of updating the trusted lists referred to in paragraph 1 of that Article and the competent authority designated or established pursuant to Article 8(1) of Directive (EU) 2022/2555.

4. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the following:

(a) the accreditation of the conformity assessment bodies and for the conformity assessment report referred to in paragraph 1;

(b) the auditing requirements for the conformity assessment bodies to carry out their conformity assessment, including composite assessment, of the qualified trust service providers as referred to in paragraph 1;

(c) the conformity assessment schemes for carrying out the conformity assessment of the qualified trust service providers by the conformity assessment bodies and for the provision of the report referred to in paragraph 1.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

▼B

Article 21

Initiation of a qualified trust service

▼M2

1. Where trust service providers intend to start providing a qualified trust service, they shall notify the supervisory body of their intention together with a conformity assessment report issued by a conformity assessment body confirming the fulfilment of the requirements laid down in this Regulation and in Article 21 of Directive (EU) 2022/2555.

2. The supervisory body shall verify whether the trust service provider and the trust services provided by it comply with the requirements laid down in this Regulation and, in particular, with the requirements for qualified trust service providers and for the qualified trust services they provide.

▼M2

In order to verify the compliance of the trust service provider with the requirements laid down in Article 21 of Directive (EU) 2022/2555, the supervisory body shall request the competent authorities designated or established pursuant to Article 8(1) of that Directive to carry out supervisory actions in that regard and to provide information about the outcome without undue delay and in any event within two months of receipt of that request. If the verification is not concluded within two months of the notification, those competent authorities shall inform the supervisory body specifying the reasons for the delay and the period within which the verification is to be concluded.

Where the supervisory body concludes that the trust service provider and the trust services provided by it comply with the requirements laid down in this Regulation, the supervisory body shall grant qualified status to the trust service provider and the trust services it provides and inform the body referred to in Article 22(3) for the purposes of updating the trusted lists referred to in Article 22(1), not later than three months after notification in accordance with paragraph 1 of this Article.

Where the verification is not concluded within three months of notification, the supervisory body shall inform the trust service provider specifying the reasons for the delay and the period within which the verification is to be concluded.

▼B

3. Qualified trust service providers may begin to provide the qualified trust service after the qualified status has been indicated in the trusted lists referred to in Article 22(1).

▼M2

4. By 21 May 2025, the Commission shall, by means of implementing acts, establish the formats and procedures of the notification and verification for the purposes of paragraphs 1 and 2 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

▼B

Article 22

Trusted lists

1. Each Member State shall establish, maintain and publish trusted lists, including information related to the qualified trust service providers for which it is responsible, together with information related to the qualified trust services provided by them.

2. Member States shall establish, maintain and publish, in a secured manner, the electronically signed or sealed trusted lists referred to in paragraph 1 in a form suitable for automated processing.

3. Member States shall notify to the Commission, without undue delay, information on the body responsible for establishing, maintaining and publishing national trusted lists, and details of where such lists are published, the certificates used to sign or seal the trusted lists and any changes thereto.

▼B

4. The Commission shall make available to the public, through a secure channel, the information referred to in paragraph 3 in electronically signed or sealed form suitable for automated processing.

5. By 18 September 2015 the Commission shall, by means of implementing acts, specify the information referred to in paragraph 1 and define the technical specifications and formats for trusted lists applicable for the purposes of paragraphs 1 to 4. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 23

EU trust mark for qualified trust services

1. After the qualified status referred to in the second subparagraph of Article 21(2) has been indicated in the trusted list referred to in Article 22(1), qualified trust service providers may use the EU trust mark to indicate in a simple, recognisable and clear manner the qualified trust services they provide.

2. When using the EU trust mark for the qualified trust services referred to in paragraph 1, qualified trust service providers shall ensure that a link to the relevant trusted list is made available on their website.

3. By 1 July 2015 the Commission shall, by means of implementing acts, provide for specifications with regard to the form, and in particular the presentation, composition, size and design of the EU trust mark for qualified trust services. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 24

Requirements for qualified trust service providers

▼M2

1. When issuing a qualified certificate or a qualified electronic attestation of attributes, a qualified trust service provider shall verify the identity and, if applicable, any specific attributes of the natural or legal person to whom the qualified certificate or the qualified electronic attestation of attributes is to be issued.

1a. The verification of the identity referred to in paragraph 1 shall be performed, by appropriate means, by the qualified trust service provider, either directly or by means of a third party, on the basis of one of the following methods or, when needed, on a combination thereof in accordance with the implementing acts referred to in paragraph 1c:

(a) by means of the European Digital Identity Wallet or a notified electronic identification means which meets the requirements set out in Article 8 with regard to assurance level high;

(b) by means of a certificate of a qualified electronic signature or of a qualified electronic seal, issued in compliance with point (a), (c) or (d);

▼M2

(c) by using other identification methods which ensure the identification of the person with a high level of confidence, the conformity of which shall be confirmed by a conformity assessment body;

(d) through the physical presence of the natural person or of an authorised representative of the legal person, by means of appropriate evidence and procedures, in accordance with national law.

1b. The verification of the attributes referred to in paragraph 1 shall be performed, by appropriate means, by the qualified trust service provider, either directly or by means of a third party, on the basis of one of the following methods or, where necessary, on a combination thereof, in accordance with the implementing acts referred to in paragraph 1c:

(a) by means of the European Digital Identity Wallet or a notified electronic identification means which meets the requirements set out in Article 8 with regard to assurance level high;

(b) by means of a certificate of a qualified electronic signature or of a qualified electronic seal, issued in accordance with paragraph 1a, point (a), (c) or (d);

(c) by means of a qualified electronic attestation of attributes;

(d) by using other methods, which ensure the verification of the attributes with a high level of confidence, the conformity of which shall be confirmed by a conformity assessment body;

(e) by means of the physical presence of the natural person or of an authorised representative of the legal person, by means of appropriate evidence and procedures, in accordance with national law.

1c. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the verification of identity and attributes in accordance with paragraphs 1, 1a and 1b of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

▼B

2. A qualified trust service provider providing qualified trust services shall:

▼M2

(a) inform the supervisory body at least one month before implementing any change in the provision of its qualified trust services or at least three months in case of an intention to cease those activities;

▼B

(b) employ staff and, if applicable, subcontractors who possess the necessary expertise, reliability, experience, and qualifications and who have received appropriate training regarding security and personal data protection rules and shall apply administrative and management procedures which correspond to European or international standards;

(c) with regard to the risk of liability for damages in accordance with Article 13, maintain sufficient financial resources and/or obtain appropriate liability insurance, in accordance with national law;

▼M2

(d) before entering into a contractual relationship, inform, in a clear, comprehensive and easily accessible manner, in a publicly accessible space and individually any person seeking to use a qualified trust service of the precise terms and conditions regarding the use of that service, including any limitations on its use;

(e) use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them, including using suitable cryptographic techniques;

▼B

(f) use trustworthy systems to store data provided to it, in a verifiable form so that:

(i) they are publicly available for retrieval only where the consent of the person to whom the data relates has been obtained,

(ii) only authorised persons can make entries and changes to the stored data,

(iii) the data can be checked for authenticity;

▼M2

(fa) notwithstanding Article 21 of Directive (EU) 2022/2555, have appropriate policies and take corresponding measures to manage legal, business, operational and other direct or indirect risks to the provision of the qualified trust service, including at least measures related to the following:

(i) registration and onboarding procedures for a service;

(ii) procedural or administrative checks;

(iii) the management and implementation of services;

(fb) notify the supervisory body, the identifiable affected individuals, other relevant competent bodies where applicable and, at the request of the supervisory body, the public if it is of public interest, of any security breaches or disruptions in the provision of the service or the implementation of the measures referred to in point (fa)(i), (ii) or (iii) that have a significant impact on the trust service provided or on the personal data maintained therein, without undue delay and in any event within 24 hours of the incident;

(g) take appropriate measures against forgery, theft or misappropriation of data or, without right, deleting, altering or rendering data inaccessible;

(h) record and keep accessible for as long as necessary after the activities of the qualified trust service provider have ceased, all relevant information concerning data issued and received by the qualified trust service provider, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service. Such recording may be done electronically;

▼M2

(i) have an up-to-date termination plan to ensure the continuity of service in accordance with provisions that are verified by the supervisory body pursuant to Article 46b(4), point (i);

_____

▼B

(k) in case of qualified trust service providers issuing qualified certificates, establish and keep updated a certificate database.

▼M2

The supervisory body may request information in addition to the information notified pursuant to point (a) of the first subparagraph or the result of a conformity assessment and may condition the granting of the permission to implement the intended changes to the qualified trust services. If the verification is not concluded within three months of notification, the supervisory body shall inform the trust service provider, specifying the reasons for the delay and the period within which the verification is to be concluded.

▼B

3. If a qualified trust service provider issuing qualified certificates decides to revoke a certificate, it shall register such revocation in its certificate database and publish the revocation status of the certificate in a timely manner, and in any event within 24 hours after the receipt of the request. The revocation shall become effective immediately upon its publication.

4. With regard to paragraph 3, qualified trust service providers issuing qualified certificates shall provide to any relying party information on the validity or revocation status of qualified certificates issued by them. This information shall be made available at least on a per certificate basis at any time and beyond the validity period of the certificate in an automated manner that is reliable, free of charge and efficient.

▼M2

4a. Paragraphs 3 and 4 shall apply accordingly to the revocation of qualified electronic attestations of attributes.

4b. The Commission shall be empowered to adopt delegated acts in accordance with Article 47, establishing additional measures referred to in paragraph 2, point (fa), of this Article.

5. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the requirements referred to in paragraph 2 of this Article. Compliance with the requirements laid down in this paragraph shall be presumed where those standards, specifications and procedures are met. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 24a

Recognition of qualified trust services

1. Qualified electronic signatures based on a qualified certificate issued in one Member State and qualified electronic seals based on a qualified certificate issued in one Member State shall be recognised,

▼M2

respectively, as qualified electronic signatures and qualified electronic seals in all other Member States.

2. Qualified electronic signature creation devices and qualified electronic seal creation devices certified in one Member State shall be recognised, respectively, as qualified electronic signature creation devices and qualified electronic seal creation devices in all other Member States.

3. A qualified certificate for electronic signatures, a qualified certificate for electronic seals, a qualified trust service for the management of remote qualified electronic signature creation devices and a qualified trust service for the management of remote qualified electronic seal creation devices provided in one Member State shall be recognised, respectively, as a qualified certificate for electronic signatures, a qualified certificate for electronic seals, a qualified trust service for the management of remote qualified electronic signature creation devices and a qualified trust service for the management of remote qualified electronic seal creation devices in all other Member States.

4. A qualified validation service for qualified electronic signatures and a qualified validation service for qualified electronic seals provided in one Member State shall be recognised, respectively, as a qualified validation service for qualified electronic signatures and a qualified validation service for qualified electronic seals in all other Member States.

5. A qualified preservation service for qualified electronic signatures and a qualified preservation service for qualified electronic seals provided in one Member State shall be recognised, respectively, as a qualified preservation service for qualified electronic signatures and a qualified preservation service for qualified electronic seals in all other Member States.

6. A qualified electronic time stamp provided in one Member State shall be recognised as a qualified electronic time stamp in all other Member States.

7. A qualified certificate for website authentication issued in one Member State shall be recognised as a qualified certificate for website authentication in all other Member States.

8. A qualified electronic registered delivery service provided in one Member State shall be recognised as a qualified electronic registered delivery service in all other Member States.

9. A qualified electronic attestation of attributes issued in one Member State shall be recognised as a qualified electronic attestation of attributes in all other Member States.

10. A qualified electronic archiving service provided in one Member State shall be recognised as a qualified electronic archiving service in all other Member States.

▼M2

11. A qualified electronic ledger provided in one Member State shall be recognised as a qualified electronic ledger in all other Member States.

▼B

SECTION 4

Electronic signatures

Article 25

Legal effects of electronic signatures

1. An electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures.

2. A qualified electronic signature shall have the equivalent legal effect of a handwritten signature.

▼M2

_____

▼B

Article 26

Requirements for advanced electronic signatures

►M2 1. ◄ An advanced electronic signature shall meet the following requirements:

(a) it is uniquely linked to the signatory;

(b) it is capable of identifying the signatory;

(c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and

(d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

▼M2

2. By 21 May 2026, the Commission shall assess whether it is necessary to adopt implementing acts to establish a list of reference standards and, where necessary, establish specifications and procedures for advanced electronic signatures. On the basis of that assessment, the Commission may adopt such implementing acts. Compliance with the requirements for advanced electronic signatures shall be presumed where an advanced electronic signature complies with the standards, specifications and procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

▼B

Article 27

Electronic signatures in public services

1. If a Member State requires an advanced electronic signature to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise advanced electronic signatures,

▼B

advanced electronic signatures based on a qualified certificate for electronic signatures, and qualified electronic signatures in at least the formats or using methods defined in the implementing acts referred to in paragraph 5.

2. If a Member State requires an advanced electronic signature based on a qualified certificate to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise advanced electronic signatures based on a qualified certificate and qualified electronic signatures in at least the formats or using methods defined in the implementing acts referred to in paragraph 5.

3. Member States shall not request for cross-border use in an online service offered by a public sector body an electronic signature at a higher security level than the qualified electronic signature.

▼M2

_____

▼B

5. By 18 September 2015, and taking into account existing practices, standards and Union legal acts, the Commission shall, by means of implementing acts, define reference formats of advanced electronic signatures or reference methods where alternative formats are used. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 28

Qualified certificates for electronic signatures

1. Qualified certificates for electronic signatures shall meet the requirements laid down in Annex I.

2. Qualified certificates for electronic signatures shall not be subject to any mandatory requirement exceeding the requirements laid down in Annex I.

3. Qualified certificates for electronic signatures may include non-mandatory additional specific attributes. Those attributes shall not affect the interoperability and recognition of qualified electronic signatures.

4. If a qualified certificate for electronic signatures has been revoked after initial activation, it shall lose its validity from the moment of its revocation, and its status shall not in any circumstances be reverted.

5. Subject to the following conditions, Member States may lay down national rules on temporary suspension of a qualified certificate for electronic signature:

(a) if a qualified certificate for electronic signature has been temporarily suspended that certificate shall lose its validity for the period of suspension;

(b) the period of suspension shall be clearly indicated in the certificate database and the suspension status shall be visible, during the period of suspension, from the service providing information on the status of the certificate.

▼M2

6. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for qualified certificates for electronic signature. Compliance with the requirements laid down in Annex I shall be presumed where a qualified certificate for electronic signature complies with those standards, specifications and procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

▼B

Article 29

Requirements for qualified electronic signature creation devices

1. Qualified electronic signature creation devices shall meet the requirements laid down in Annex II.

▼M2

1a. Generating or managing electronic signature creation data or duplicating such signature creation data for back-up purposes shall be carried out only on behalf of the signatory, at the request of the signatory, and by a qualified trust service provider providing a qualified trust service for the management of a remote qualified electronic signature creation device.

▼B

2. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified electronic signature creation devices. Compliance with the requirements laid down in Annex II shall be presumed where a qualified electronic signature creation device meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

▼M2

Article 29a

Requirements for a qualified service for the management of remote qualified electronic signature creation devices

1. The management of remote qualified electronic signature creation devices as a qualified service shall be carried out only by a qualified trust service provider that:

(a) generates or manages electronic signature creation data on behalf of the signatory;

(b) notwithstanding point (1)(d) of Annex II, duplicates the electronic signature creation data for back-up purposes only, provided that the following requirements are met:

(i) the security of the duplicated datasets must be at the same level as for the original datasets;

(ii) the number of duplicated datasets must not exceed the minimum needed to ensure continuity of the service;

▼M2

(c) complies with any requirements identified in the certification report of the specific remote qualified electronic signature creation device issued pursuant to Article 30.

2. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, specifications and procedures for the purposes of paragraph 1 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

▼B

Article 30

Certification of qualified electronic signature creation devices

1. Conformity of qualified electronic signature creation devices with the requirements laid down in Annex II shall be certified by appropriate public or private bodies designated by Member States.

2. Member States shall notify to the Commission the names and addresses of the public or private body referred to in paragraph 1. The Commission shall make that information available to Member States.

3. The certification referred to in paragraph 1 shall be based on one of the following:

(a) a security evaluation process carried out in accordance with one of the standards for the security assessment of information technology products included in the list established in accordance with the second subparagraph; or

(b) a process other than the process referred to in point (a), provided that it uses comparable security levels and provided that the public or private body referred to in paragraph 1 notifies that process to the Commission. That process may be used only in the absence of standards referred to in point (a) or when a security evaluation process referred to in point (a) is ongoing.

The Commission shall, by means of implementing acts, establish a list of standards for the security assessment of information technology products referred to in point (a). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

▼M2

3a The validity of a certification referred to in paragraph 1 shall not exceed five years, provided that vulnerabilities assessments are carried out every two years. Where vulnerabilities are identified and not remedied, the certification shall be cancelled.

▼B

4. The Commission shall be empowered to adopt delegated acts in accordance with Article 47 concerning the establishment of specific criteria to be met by the designated bodies referred to in paragraph 1 of this Article.

▼B

Article 31

Publication of a list of certified qualified electronic signature creation devices

1. Member States shall notify to the Commission without undue delay and no later than one month after the certification is concluded, information on qualified electronic signature creation devices that have been certified by the bodies referred to in Article 30(1). They shall also notify to the Commission, without undue delay and no later than one month after the certification is cancelled, information on electronic signature creation devices that are no longer certified.

2. On the basis of the information received, the Commission shall establish, publish and maintain a list of certified qualified electronic signature creation devices.

▼M2

3. By 21 May 2025, the Commission shall, by means of implementing acts, establish the formats and procedures applicable for the purpose of paragraph 1 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

▼B

Article 32

Requirements for the validation of qualified electronic signatures

1. The process for the validation of a qualified electronic signature shall confirm the validity of a qualified electronic signature provided that:

(a) the certificate that supports the signature was, at the time of signing, a qualified certificate for electronic signature complying with Annex I;

(b) the qualified certificate was issued by a qualified trust service provider and was valid at the time of signing;

(c) the signature validation data corresponds to the data provided to the relying party;

(d) the unique set of data representing the signatory in the certificate is correctly provided to the relying party;

(e) the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing;

(f) the electronic signature was created by a qualified electronic signature creation device;

(g) the integrity of the signed data has not been compromised;

(h) the requirements provided for in Article 26 were met at the time of signing.

▼M2

Compliance with the requirements laid down in the first subparagraph of this paragraph shall be presumed where the validation of qualified electronic signatures complies with the standards, specifications and procedures referred to in paragraph 3.

▼B

2. The system used for validating the qualified electronic signature shall provide to the relying party the correct result of the validation process and shall allow the relying party to detect any security relevant issues.

▼M2

3. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the validation of qualified electronic signatures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 32a

Requirements for the validation of advanced electronic signatures based on qualified certificates

1. The process for the validation of an advanced electronic signature based on a qualified certificate shall confirm the validity of an advanced electronic signature based on a qualified certificate, provided that:

(a) the certificate that supports the signature was, at the time of signing, a qualified certificate for electronic signature complying with Annex I;

(b) the qualified certificate was issued by a qualified trust service provider and was valid at the time of signing;

(c) the signature validation data corresponds to the data provided to the relying party;

(d) the unique set of data representing the signatory in the certificate is correctly provided to the relying party;

(e) the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing;

(f) the integrity of the signed data has not been compromised;

(g) the requirements provided for in Article 26 were met at the time of signing.

2. The system used for validating the advanced electronic signature based on qualified certificate shall provide to the relying party the correct result of the validation process and shall allow the relying party to detect any security relevant issues.

3. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the validation of advanced electronic signatures based on qualified certificates. Compliance with the requirements laid down in paragraph 1 of this Article shall be presumed where the validation of advanced electronic signature based on qualified certificates complies with those standards, specifications and procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

▼B

Article 33

Qualified validation service for qualified electronic signatures

1. A qualified validation service for qualified electronic signatures may only be provided by a qualified trust service provider who:

(a) provides validation in compliance with Article 32(1); and

(b) allows relying parties to receive the result of the validation process in an automated manner, which is reliable, efficient and bears the advanced electronic signature or advanced electronic seal of the provider of the qualified validation service.

▼M2

2. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for qualified validation service referred to in paragraph 1 of this Article. Compliance with the requirements laid down in paragraph 1 of this Article shall be presumed where the qualified validation service for qualified electronic signatures complies with those standards, specifications and procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

▼B

Article 34

Qualified preservation service for qualified electronic signatures

1. A qualified preservation service for qualified electronic signatures may only be provided by a qualified trust service provider that uses procedures and technologies capable of extending the trustworthiness of the qualified electronic signature beyond the technological validity period.

▼M2

1a. Compliance with the requirements laid down in paragraph 1 shall be presumed where the arrangements for the qualified preservation service for qualified electronic signatures complies with the standards, specifications and procedures referred to in paragraph 2.

2. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the qualified preservation service for qualified electronic signatures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

▼B

SECTION 5

Electronic seals

Article 35

Legal effects of electronic seals

1. An electronic seal shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic seals.

2. A qualified electronic seal shall enjoy the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked.

▼M2

_____

▼B

Article 36

Requirements for advanced electronic seals

►M2 1. ◄ An advanced electronic seal shall meet the following requirements:

(a) it is uniquely linked to the creator of the seal;

(b) it is capable of identifying the creator of the seal;

(c) it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation; and

(d) it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable.

▼M2

2. By 21 May 2026, the Commission shall assess whether it is necessary to adopt implementing acts to establish a list of reference standards and, where necessary, establish specifications and procedures for advanced electronic seals. On the basis of that assessment, the Commission may adopt such implementing acts. Compliance with the requirements for advanced electronic seals shall be presumed where an advanced electronic seal complies with those standards, specifications and procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

▼B

Article 37

Electronic seals in public services

1. If a Member State requires an advanced electronic seal in order to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise advanced electronic seals, advanced electronic seals based on a qualified certificate for electronic seals and qualified electronic seals at least in the formats or using methods defined in the implementing acts referred to in paragraph 5.

▼B

2. If a Member State requires an advanced electronic seal based on a qualified certificate in order to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise advanced electronic seals based on a qualified certificate and qualified electronic seal at least in the formats or using methods defined in the implementing acts referred to in paragraph 5.

3. Member States shall not request for the cross-border use in an online service offered by a public sector body an electronic seal at a higher security level than the qualified electronic seal.

▼M2

_____

▼B

5. By 18 September 2015, and taking into account existing practices, standards and legal acts of the Union, the Commission shall, by means of implementing acts, define reference formats of advanced electronic seals or reference methods where alternative formats are used. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 38

Qualified certificates for electronic seals

1. Qualified certificates for electronic seals shall meet the requirements laid down in Annex III.

2. Qualified certificates for electronic seals shall not be subject to any mandatory requirements exceeding the requirements laid down in Annex III.

3. Qualified certificates for electronic seals may include non-mandatory additional specific attributes. Those attributes shall not affect the interoperability and recognition of qualified electronic seals.

4. If a qualified certificate for an electronic seal has been revoked after initial activation, it shall lose its validity from the moment of its revocation, and its status shall not in any circumstances be reverted.

5. Subject to the following conditions, Member States may lay down national rules on temporary suspension of qualified certificates for electronic seals:

(a) if a qualified certificate for electronic seal has been temporarily suspended, that certificate shall lose its validity for the period of suspension;

(b) the period of suspension shall be clearly indicated in the certificate database and the suspension status shall be visible, during the period of suspension, from the service providing information on the status of the certificate.

▼M2

6. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for qualified certificates for electronic seals. Compliance with the requirements laid down in Annex III shall be presumed where a qualified certificate for electronic seal complies with those standards, specifications and procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

▼B

Article 39

Qualified electronic seal creation devices

1. Article 29 shall apply mutatis mutandis to requirements for qualified electronic seal creation devices.

2. Article 30 shall apply mutatis mutandis to the certification of qualified electronic seal creation devices.

3. Article 31 shall apply mutatis mutandis to the publication of a list of certified qualified electronic seal creation devices.

▼M2

Article 39a

Requirements for a qualified service for the management of remote qualified electronic seal creation devices

Article 29a shall apply *mutatis mutandis* to a qualified service for the management of remote qualified electronic seal creation devices.

▼B

Article 40

Validation and preservation of qualified electronic seals

Articles 32, 33 and 34 shall apply mutatis mutandis to the validation and preservation of qualified electronic seals.

▼M2

Article 40a

Requirements for the validation of advanced electronic seals based on qualified certificates

Article 32a shall apply *mutatis mutandis* to the validation of advanced electronic seals based on qualified certificates.

▼B

SECTION 6

Electronic time stamps

Article 41

Legal effect of electronic time stamps

1. An electronic time stamp shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic time stamp.

2. A qualified electronic time stamp shall enjoy the presumption of the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound.

▼M2

_____

▼B

Article 42

Requirements for qualified electronic time stamps

1. A qualified electronic time stamp shall meet the following requirements:

(a) it binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably;

(b) it is based on an accurate time source linked to Coordinated Universal Time; and

(c) it is signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider, or by some equivalent method.

▼M2

1a. Compliance with the requirements laid down in paragraph 1 shall be presumed where the binding of date and time to data and the accuracy of the time source comply with the standards, specifications and procedures referred to in paragraph 2.

2. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the binding of date and time to data and for establishing the accuracy of time sources. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

▼B

SECTION 7

Electronic registered delivery services

Article 43

Legal effect of an electronic registered delivery service

1. Data sent and received using an electronic registered delivery service shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic registered delivery service.

2. Data sent and received using a qualified electronic registered delivery service shall enjoy the presumption of the integrity of the data, the sending of that data by the identified sender, its receipt by the identified addressee and the accuracy of the date and time of sending and receipt indicated by the qualified electronic registered delivery service.

Article 44

Requirements for qualified electronic registered delivery services

1. Qualified electronic registered delivery services shall meet the following requirements:

▼B

(a) they are provided by one or more qualified trust service provider (s);

(b) they ensure with a high level of confidence the identification of the sender;

(c) they ensure the identification of the addressee before the delivery of the data;

(d) the sending and receiving of data is secured by an advanced electronic signature or an advanced electronic seal of a qualified trust service provider in such a manner as to preclude the possibility of the data being changed undetectably;

(e) any change of the data needed for the purpose of sending or receiving the data is clearly indicated to the sender and addressee of the data;

(f) the date and time of sending, receiving and any change of data are indicated by a qualified electronic time stamp.

In the event of the data being transferred between two or more qualified trust service providers, the requirements in points (a) to (f) shall apply to all the qualified trust service providers.

▼M2

1a. Compliance with the requirements laid down in paragraph 1 shall be presumed where the process for sending and receiving data complies with the standards, specifications and procedures referred to in paragraph 2.

2. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for processes for sending and receiving data. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

2a. Providers of qualified electronic registered delivery services may agree on interoperability between qualified electronic registered delivery services which they provide. Such interoperability framework shall comply with the requirements laid down in paragraph 1 and such compliance shall be confirmed by a conformity assessment body.

2b. The Commission may, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the interoperability framework referred to in paragraph 2a of this Article. The technical specifications and content of standards shall be cost-effective and proportionate. The implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

▼B

SECTION 8

Website authentication

▼M2

Article 45

Requirements for qualified certificates for website authentication

1. Qualified certificates for website authentication shall meet the requirements laid down in Annex IV. The evaluation of compliance with those requirements shall be carried out in accordance with the standards, specifications and procedures referred to in paragraph 2 of this Article.

1a. Qualified certificates for website authentication issued in accordance with paragraph 1 of this Article shall be recognised by providers of web-browsers. Providers of web-browsers shall ensure that the identity data attested in the certificate and additional attested attributes are displayed in a user-friendly manner. Providers of web-browsers shall ensure support and interoperability with qualified certificates for website authentication referred to in paragraph 1 of this Article, with the exception of microenterprises or small enterprises as defined in Article 2 of the Annex to Recommendation 2003/361/EC during the first five years of operating as providers of web-browsing services.

1b. Qualified certificates for website authentication shall not be subject to any mandatory requirements other than the requirements laid down in paragraph 1.

2. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for qualified certificates for website authentication, referred to in paragraph 1 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 45a

Cybersecurity precautionary measures

1. Providers of web-browsers shall not take any measures contrary to their obligations set out in Article 45, in particular the requirements to recognise qualified certificates for website authentication and to display the identity data provided in a user-friendly manner.

2. By way of derogation from paragraph 1 and only in the event of substantiated concerns related to security breaches or the loss of integrity of an identified certificate or set of certificates, providers of web-browsers may take precautionary measures in relation to that certificate or set of certificates.

3. Where a provider of a web-browser takes precautionary measures pursuant to paragraph 2, the provider of the web-browser shall notify its concerns in writing, without undue delay, together with a description of the measures taken to mitigate those concerns, to the Commission, the competent supervisory body, the entity to whom the certificate was

▼M2

issued and to the qualified trust service provider that issued that certificate or set of certificates. Upon receipt of such a notification, the competent supervisory body shall issue an acknowledgement of receipt to the provider of the web-browser in question.

4. The competent supervisory body shall investigate the issues raised in the notification in accordance with Article 46b(4), point (k). Where the outcome of that investigation does not result in the withdrawal of the qualified status of the certificate, the supervisory body shall inform the provider of the web-browser accordingly and shall request that provider to put an end to the precautionary measures referred to in paragraph 2 of this Article.

SECTION 9

electronic attestation of attributes

Article 45b

Legal effects of electronic attestation of attributes

1. An electronic attestation of attributes shall not be denied legal effect or admissibility as evidence in legal proceedings on the sole ground that it is in electronic form or that it does not meet the requirements for qualified electronic attestations of attributes.

2. A qualified electronic attestation of attributes and attestations of attributes issued by, or on behalf of, a public sector body responsible for an authentic source shall have the same legal effect as lawfully issued attestations in paper form.

3. An attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source in one Member State shall be recognised as an attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source in all Member States.

Article 45c

Electronic attestation of attributes in public services

Where an electronic identification using an electronic identification means and authentication is required under national law to access an online service provided by a public sector body, person identification data in the electronic attestation of attributes shall not substitute electronic identification using an electronic identification means and authentication for electronic identification unless specifically allowed by the Member State. In such a case, qualified electronic attestation of attributes from other Member States shall also be accepted.

Article 45d

Requirements for qualified electronic attestation of attributes

1. Qualified electronic attestation of attributes shall meet the requirements laid down in Annex V.

▼M2

2. The evaluation of compliance with the requirements laid down in Annex V shall be carried out in accordance with the standards, specifications and procedures referred to in paragraph 5 of this Article.

3. Qualified electronic attestations of attributes shall not be subject to any mandatory requirement in addition to the requirements laid down in Annex V.

4. Where a qualified electronic attestation of attributes has been revoked after initial issuance, it shall lose its validity from the moment of its revocation and its status shall not in any circumstances be reverted.

5. By 21 November 2024, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for qualified electronic attestations of attributes. Those implementing acts shall be consistent with the implementing acts referred to in Article 5a(23) on the implementation of the European Digital Identity Wallet. They shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 45e

Verification of attributes against authentic sources

1. Member States shall ensure, within 24 months of the date of entry into force of the implementing acts referred to in Articles 5a(23) and 5c (6), that, at least for the attributes listed in Annex VI, wherever those attributes rely on authentic sources within the public sector, measures are taken to allow qualified trust service providers of electronic attestations of attributes to verify those attributes by electronic means at the request of the user, in accordance with Union or national law.

2. By 21 November 2024, the Commission shall, taking into account relevant international standards, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the catalogue of attributes, as well as schemes for the attestation of attributes and verification procedures for qualified electronic attestations of attributes for the purposes of paragraph 1 of this Article. Those implementing acts shall be consistent with the implementing acts referred to in Article 5a(23) on the implementation of the European Digital Identity Wallet. They shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 45f

Requirements for electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source

1. An electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source shall meet the following requirements:

(a) those set out in Annex VII;

▼M2

(b) the qualified certificate supporting the qualified electronic signature or qualified electronic seal of the public sector body referred to in Article 3, point (46), identified as the issuer referred to in point (b), of Annex VII, containing a specific set of certified attributes in a form suitable for automated processing and:

(i) indicating that the issuing body is established in accordance with Union or national law as the responsible for the authentic source on the basis of which the electronic attestation of attributes is issued or as the body designated to act on its behalf;

(ii) providing a set of data unambiguously representing the authentic source referred to in point (i); and

(iii) identifying the Union or national law referred to in point (i).

2. The Member State where public sector bodies referred to in Article 3, point (46), are established shall ensure that the public sector bodies that issue electronic attestations of attributes meet a level of reliability and trustworthiness equivalent to qualified trust service providers in accordance with Article 24.

3. Member States shall notify public sector bodies referred to in Article 3, point (46), to the Commission. That notification shall include a conformity assessment report issued by a conformity assessment body confirming that the requirements set out in paragraphs 1, 2 and 6 of this Article are met. The Commission shall make available to the public, through a secure channel, the list of public sector bodies referred to in Article 3, point (46), in electronically signed or sealed form suitable for automated processing.

4. Where an electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source has been revoked after initial issuance, it shall lose its validity from the moment of its revocation and its status shall not be reverted.

5. An electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source shall be deemed to be compliant with the requirements laid down in paragraph 1, where it complies with the standards, specifications and procedures referred to in paragraph 6.

6. By 21 November 2024, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source. Those implementing acts shall be consistent with the implementing acts referred to in Article 5a(23) on the implementation of the European Digital Identity Wallet. They shall be adopted in accordance with the examination procedure referred to in Article 48(2).

▼M2

7. By 21 November 2024, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the purposes of paragraph 3 of this Article. Those implementing acts shall be consistent with the implementing acts referred to in Article 5a(23) on the implementation of the European Digital Identity Wallet. They shall be adopted in accordance with the examination procedure referred to in Article 48(2).

8. Public sector bodies referred to in Article 3, point (46), issuing electronic attestation of attributes shall provide an interface with European Digital Identity Wallets that are provided in accordance with Article 5a.

Article 45g

Issuing of electronic attestation of attributes to European Digital Identity Wallets

1. Providers of electronic attestations of attributes shall provide European Digital Identity Wallet users with the possibility to request, obtain, store and manage the electronic attestation of attributes irrespective of the Member State where the European Digital Identity Wallet is provided.

2. Providers of qualified electronic attestations of attributes shall provide an interface with European Digital Identity Wallets that are provided in accordance in Article 5a.

Article 45h

Additional rules for the provision of electronic attestation of attributes services

1. Providers of qualified and non-qualified electronic attestation of attributes services shall not combine personal data relating to the provision of those services with personal data from any other services offered by them or their commercial partners.

2. Personal data relating to the provision of electronic attestation of attributes services shall be kept logically separate from other data held by the provider of electronic attestation of attributes.

3. Providers of qualified electronic attestation of attributes' services shall implement the provision of such qualified trust services in a manner that is functionally separate from other services provided by them.

SECTION 10

electronic archiving services

Article 45i

Legal effect of electronic archiving services

1. Electronic data and electronic documents preserved using an electronic archiving service shall not be denied legal effect or admissibility as evidence in legal proceedings on the sole ground that they are in

▼M2

electronic form or that they are not preserved using a qualified electronic archiving service.

2. Electronic data and electronic documents preserved using a qualified electronic archiving service shall enjoy the presumption of their integrity and of their origin for the duration of the preservation period by the qualified trust service provider.

Article 45j

Requirements for qualified electronic archiving services

1. Qualified electronic archive services shall meet the following requirements:

(a) they are provided by qualified trust service providers;

(b) they use procedures and technologies capable of ensuring the durability and legibility of electronic data and electronic documents beyond the technological validity period and at least throughout the legal or contractual preservation period, while maintaining their integrity and the accuracy of their origin;

(c) they ensure that those electronic data and those electronic documents are preserved in such a way that they are safeguarded against loss and alteration, except for changes concerning their medium or electronic format;

(d) they shall allow authorised relying parties to receive a report in an automated manner that confirms that electronic data and electronic documents retrieved from a qualified electronic archive enjoy the presumption of integrity of the data from the beginning of the preservation period to the moment of retrieval.

The report referred to in point (d) of the first subparagraph shall be provided in a reliable and efficient way and shall bear the qualified electronic signature or qualified electronic seal of the provider of the qualified electronic archiving service.

2. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for qualified electronic archiving services. Compliance with the requirements for qualified electronic archive services shall be presumed where a qualified electronic archive service complies with those standards, specifications and procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

SECTION 11

electronic ledgers

Article 45k

Legal effects of electronic ledgers

1. An electronic ledger shall not be denied legal effect or admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic ledgers.

▼M2

2. Data records contained in a qualified electronic ledger shall enjoy the presumption of their unique and accurate sequential chronological ordering and of their integrity.

Article 45l

Requirements for qualified electronic ledgers

1. Qualified electronic ledgers shall meet the following requirements:

(a) they are created and managed by one or more qualified trust service providers;

(b) they establish the origin of data records in the ledger;

(c) they ensure the unique sequential chronological ordering of data records in the ledger;

(d) they record data in such a way that any subsequent change to the data is immediately detectable, ensuring their integrity over time.

2. Compliance with the requirements laid down in paragraph 1 shall be presumed where an electronic ledger complies with the standards, specifications and procedures referred to in paragraph 3.

3. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the requirements laid down in paragraph 1 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

▼B

CHAPTER IV

ELECTRONIC DOCUMENTS

Article 46

Legal effects of electronic documents

An electronic document shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form.

▼M2

CHAPTER IVa

GOVERNANCE FRAMEWORK

Article 46a

Supervision of the European Digital Identity Wallet Framework

1. Member States shall designate one or more supervisory bodies established in their territory.

The supervisory bodies designated pursuant to the first subparagraph shall be given the necessary powers and adequate resources for the exercise of their tasks in an effective, efficient and independent manner.

▼M2

2. Member States shall notify to the Commission the names and the addresses of their supervisory bodies designated pursuant to paragraph 1 and any subsequent changes thereto. The Commission shall publish a list of the notified supervisory bodies.

3. The role of the supervisory bodies designated pursuant to paragraph 1 shall be:

(a) to supervise providers of European Digital Identity Wallets established in the designating Member State and to ensure, by means of *ex ante* and *ex post* supervisory activities, that those providers and European Digital Identity Wallets they provide meet the requirements laid down in this Regulation;

(b) to take action, if necessary, in relation to providers of European Digital Identity Wallets established in the territory of the designating Member State, by means of *ex post* supervisory activities, when informed that providers or European Digital Identity Wallets that they provide infringe this Regulation.

4. The tasks of the supervisory bodies designated pursuant to paragraph 1 shall include, in particular, the following:

(a) to cooperate with other supervisory bodies and to provide them with assistance in accordance with Articles 46c and 46e;

(b) to request information necessary to monitor compliance with this Regulation;

(c) to inform the relevant competent authorities designated or established pursuant to Article 8(1) of Directive (EU) 2022/2555 of the Member States concerned of any significant security breaches or loss of integrity of which they become aware in the performance of their tasks and, in the case of a significant security breach or loss of integrity which concerns other Member States, to inform the single point of contact designated or established pursuant to Article 8(3) of Directive (EU) 2022/2555 of the Member State concerned and the single points of contact designated pursuant to Article 46c(1) of this Regulation in the other Member States concerned, and to inform the public or require providers of European Digital Identity Wallet to do so where the supervisory body determines that disclosure of the security breach or of the loss of integrity would be in the public interest;

(d) to carry out on-site inspections and off-site supervision;

(e) to require that providers of European Digital Identity Wallets remedy any failure to fulfil the requirements laid down in this Regulation;

(f) to suspend or cancel the registration and inclusion of relying parties in the mechanism referred to in Article 5b(7) in the case of illegal or fraudulent use of the European Digital Identity Wallet;

(g) 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.

▼M2

5. Where the supervisory body designated pursuant to paragraph 1 requires the provider of a European Digital Identity Wallet to remedy any failure to fulfil requirements under this Regulation pursuant to paragraph 4, point (e), and that provider does not act accordingly and, if applicable, within a time limit set by that supervisory body, the supervisory body designated pursuant to paragraph 1 may, taking into account, in particular, the extent, duration and consequences of that failure, order the provider to suspend or to cease the provision of the European Digital Identity Wallet. The supervisory body shall inform the supervisory bodies of other Member States, the Commission, relying parties and users of the European Digital Identity Wallet without undue delay of the decision to require the suspension or cessation of the provision of the European Digital Identity Wallet.

6. By 31 March each year, each supervisory body designated pursuant to paragraph 1 shall submit to the Commission a report on its main activities in the previous calendar year. The Commission shall make those annual reports available to the European Parliament and the Council.

7. By 21 May 2025, the Commission shall, by means of implementing acts, establish the formats and procedures for the report referred to in paragraph 6 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 46b

Supervision of trust services

1. Member States shall designate a supervisory body established in their territory or designate, upon mutual agreement with another Member State, a supervisory body established in that other Member State. That supervisory body shall be responsible for supervisory tasks in the designating Member State as regards trust services.

The supervisory bodies designated pursuant to the first subparagraph shall be given the necessary powers and adequate resources for the exercise of their tasks.

2. Member States shall notify to the Commission the names and addresses of their supervisory bodies designated pursuant to paragraph 1 and any subsequent changes thereto. The Commission shall publish a list of the notified supervisory bodies.

3. The role of the supervisory bodies designated pursuant to paragraph 1 shall be:

(a) to supervise qualified trust service providers established in the territory of the designating Member State and to ensure, by means of *ex ante* and *ex post* supervisory activities, that those qualified trust service providers and the qualified trust services that they provide meet the requirements laid down in this Regulation;

(b) to take action, if necessary, in relation to non-qualified trust service providers established in the territory of the designating Member State, by means of *ex post* supervisory activities, when informed that those non-qualified trust service providers or the trust services they provide allegedly do not meet the requirements laid down in this Regulation.

▼M2

4. The tasks of the supervisory body designated pursuant to paragraph 1 shall include in particular the following:

(a) to inform the relevant competent authorities designated or established pursuant to Article 8(1) of Directive (EU) 2022/2555 of the Member States concerned of any significant security breach or loss of integrity of which it becomes aware in the performance of its tasks and, in the case of a significant security breach or loss of integrity which concerns other Member States, to inform the single point of contact designated or established pursuant to Article 8(3) Directive (EU) 2022/2555 of the Member State concerned and the single points of contact designated pursuant to Article 46c(1) of this Regulation in the other Member States concerned, and to inform the public or require the trust service provider to do so where the supervisory body determines that disclosure of the breach of security or loss of integrity would be in the public interest;

(b) to cooperate with other supervisory bodies and to provide them with assistance in accordance with Articles 46c and 46e;

(c) to analyse the conformity assessment reports referred to in Article 20(1) and Article 21(1);

(d) to report to the Commission about its main activities in accordance with paragraph 6 of this Article;

(e) to carry out audits or request a conformity assessment body to perform a conformity assessment of the qualified trust service providers in accordance with Article 20(2);

(f) 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 breached and about security breaches which appear to constitute personal data breaches;

(g) to grant qualified status to trust service providers and to the services they provide, and to withdraw that status in accordance with Articles 20 and 21;

(h) to inform the body responsible for the national trusted list referred to in Article 22(3) of its decisions to grant or withdraw qualified status, unless that body is also the supervisory body designated pursuant to paragraph 1 of this Article;

(i) to verify the existence and correct application of provisions on termination plans where the qualified trust service provider ceases its activities, including how information is kept accessible in accordance with Article 24(2), point (h);

(j) to require that trust service providers remedy any failure to fulfil the requirements laid down in this Regulation;

▼M2

(k) to investigate claims made by providers of web-browsers pursuant to Article 45a and to take action if necessary.

5. Member States may require the supervisory body designated pursuant to paragraph 1 to establish, maintain and update a trust infrastructure in accordance with national law.

6. By 31 March each year, each supervisory body designated pursuant to paragraph 1 shall submit to the Commission a report on its main activities in the previous calendar year. The Commission shall make those annual reports available to the European Parliament and the Council.

7. By 21 May 2025, the Commission shall adopt guidelines on the exercise by the supervisory bodies designated pursuant to paragraph 1 of this Article of the tasks referred to in paragraph 4 of this Article, and, by means of implementing acts, establish the formats and procedures for the report referred to in paragraph 6 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 46c

Single points of contact

1. Each Member State shall designate a single point of contact for trust services, European Digital Identity Wallets and notified electronic identification schemes.

2. Each single point of contact shall exercise a liaison function to facilitate cross-border cooperation between the supervisory bodies for trust service providers and between the supervisory bodies for the providers of European Digital Identity Wallets and, where appropriate, with the Commission and European Union Agency for Cybersecurity (ENISA) and with other competent authorities within its Member State.

3. Each Member State shall make public and, without undue delay, notify to the Commission the names and the addresses of the single point of contact designated pursuant to paragraph 1 and any subsequent change thereto.

4. The Commission shall publish a list of the single points of contact notified pursuant to paragraph 3.

Article 46d

Mutual assistance

1. In order to facilitate the supervision and enforcement of obligations under this Regulation, the supervisory bodies designated pursuant to Article 46a(1) and Article 46b(1) may seek, including through the Cooperation Group established pursuant to Article 46e (1), mutual assistance from the supervisory bodies of another Member State where the provider of the European Digital Identity Wallet or the trust service provider is established, or where its network and information systems are located or its services are provided.

2. The mutual assistance shall at least entail that:

▼M2

(a) the supervisory body applying supervisory and enforcement measures in one Member State shall inform and consult the supervisory body from the other Member State concerned;

(b) a supervisory body may request the supervisory body of another Member State concerned to take supervisory or enforcement measures, including, for instance, requests to carry out inspections related to the conformity assessment reports as referred to in Articles 20 and 21 regarding the provision of trust services;

(c) where appropriate, supervisory bodies may carry out joint investigations with the supervisory bodies of other Member States.

The arrangements and procedures for joint actions under the first subparagraph shall be agreed upon and established by the Member States concerned in accordance with their national law.

3. A supervisory body to which a request for assistance is addressed may refuse that request on any of the following grounds:

(a) the assistance requested is not proportionate to the supervisory activities of the supervisory body carried out in accordance with Articles 46a and 46b;

(b) the supervisory body is not competent to provide the requested assistance;

(c) providing the requested assistance would be incompatible with this Regulation.

4. By 21 May 2025 and every two years thereafter, the Cooperation Group established pursuant to Article 46e(1) shall issue guidance on the organisational aspects and procedures for the mutual assistance referred to in paragraphs 1 and 2 of this Article.

Article 46e

The European Digital Identity Cooperation Group

1. In order to support and facilitate Member States' cross-border cooperation and exchange of information on trust services, European Digital Identity Wallets and notified electronic identification schemes, the Commission shall establish a European Digital Identity Cooperation Group (the 'Cooperation Group').

2. The Cooperation Group shall be composed of representatives appointed by the Member States and of the Commission. The Cooperation Group shall be chaired by the Commission. The Commission shall provide the Cooperation Group's Secretariat.

3. Representatives of relevant stakeholders may, on an ad hoc basis, be invited to attend meetings of the Cooperation Group and to participate in its work as observers.

4. ENISA shall be invited to participate as observer in the workings of the Cooperation Group when it exchanges views, best practices and information on relevant cybersecurity aspects such as notification of security breaches, and when the use of cybersecurity certificates or standards are addressed.

5. The Cooperation Group shall have the following tasks:

▼M2

(a) exchange advice and cooperate with the Commission on emerging policy initiatives in the field of digital identity wallets, electronic identification means and trust services;

(b) advise the Commission, as appropriate, in the early preparation of draft implementing and delegated acts to be adopted pursuant to this Regulation;

(c) in order to support the supervisory bodies in the implementation of the provisions of this Regulation:

(i) exchange best practices and information regarding the implementation of the provisions of this Regulation;

(ii) assess the relevant developments in the digital identity wallet, electronic identification and trust services sectors;

(iii) organise joint meetings with relevant interested parties from across the Union to discuss activities carried out by the cooperation group and gather input on emerging policy challenges;

(iv) with the support of ENISA, exchange views, best practices and information on relevant cybersecurity aspects concerning European Digital Identity Wallets, electronic identification schemes and trust services;

(v) exchange best practices in relation to the development and implementation of policies on the notification of security breaches, and common measures as referred to in Articles 5e and 10;

(vi) organise joint meetings with the NIS Cooperation Group established pursuant to Article 14(1) of Directive (EU) 2022/2555 to exchange relevant information in relation to trust services and electronic identification related cyber threats, incidents, vulnerabilities, awareness raising initiatives, trainings, exercises and skills, capacity building, standards and technical specifications capacity as well as standards and technical specifications;

(vii) discuss, upon a request of a supervisory body, specific requests for mutual assistance as referred to in Article 46d;

(viii) facilitate the exchange of information between the supervisory bodies by providing guidance on the organisational aspects and procedures for the mutual assistance referred to in Article 46d;

(d) organise peer reviews of electronic identification schemes to be notified under this Regulation.

6. Member States shall ensure effective and efficient cooperation of their designated representatives in the Cooperation Group.

▼M2

7. By 21 May 2025, the Commission shall, by means of implementing acts, establish the necessary procedural arrangements to facilitate the cooperation between the Member States referred to in paragraph 5, point (d), of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

▼B

CHAPTER V

DELEGATIONS OF POWER AND IMPLEMENTING PROVISIONS

Article 47

Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

▼M2

2. The power to adopt delegated acts referred to in Article 5c(7), Article 24(4b) and Article 30(4) shall be conferred on the Commission for an indeterminate period of time from 17 September 2014.

3. The delegation of power referred to in Article 5c(7), Article 24 (4b) and Article 30(4) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

▼B

4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

▼M2

5. A delegated act adopted pursuant to Article 5c(7), Article 24(4b) or Article 30(4) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

▼B

Article 48

Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

▼B

CHAPTER VI

FINAL PROVISIONS

▼M2

Article 48a

Reporting requirements

1. Member States shall ensure the collection of statistics in relation to the functioning of European Digital Identity Wallets and the qualified trust services provided on their territory.

2. The statistics collected in accordance with paragraph 1 shall include the following:

(a) the number of natural and legal persons having a valid European Digital Identity Wallet;

(b) the type and number of services accepting the use of the European Digital Identity Wallet;

(c) the number of user complaints and consumer protection or data protection incidents relating to relying parties and qualified trust services;

(d) a summary report including data on incidents preventing the use of the European Digital Identity Wallet;

(e) a summary of significant security incidents, data breaches and affected users of European Digital Identity Wallets or of qualified trust services.

3. The statistics referred to in paragraph 2 shall be made available to the public in an open and commonly used, machine-readable format.

4. By 31 March each year, Member States shall submit to the Commission a report on the statistics collected in accordance with paragraph 2.

Article 49

Review

1. The Commission shall review the application of this Regulation and shall, by 21 May 2026, submit a report to the European Parliament and to the Council. In that report, the Commission shall, in particular, evaluate whether it is appropriate to modify the scope of this Regulation or its specific provisions including, in particular, the provisions included in Article 5c(5), taking into account the experience gained in the application of this Regulation, as well as technological, market and legal developments. Where necessary, that report shall be accompanied by a proposal to amend this Regulation.

2. The report referred to in paragraph 1 shall include an assessment of the availability, security and usability of the notified electronic identification means and European Digital Identity Wallets that fall within the scope of this Regulation and assess whether all online

▼M2

private service providers relying on third-party electronic identification services for users authentication, shall be required to accept the use of notified electronic identification means and European Digital Identity Wallet.

3. By 21 May 2030 and every four years thereafter, the Commission shall submit a report to the European Parliament and the Council on progress made towards achieving the objectives of this Regulation.

▼B

Article 50

Repeal

1. Directive 1999/93/EC is repealed with effect from 1 July 2016.

2. References to the repealed Directive shall be construed as references to this Regulation.

▼M2

Article 51

Transitional measures

1. Secure signature creation devices of which the conformity has been determined in accordance with Article 3(4) of Directive 1999/93/EC shall continue to be considered to be qualified electronic signature creation devices under this Regulation until 21 May 2027.

2. Qualified certificates issued to natural persons under Directive 1999/93/EC shall continue to be considered as qualified certificates for electronic signatures under this Regulation until 21 May 2026.

3. The management of remote qualified electronic signature and seal creation devices by qualified trust service providers other than qualified trust service providers providing qualified trust services for the management of remote qualified electronic signature and seal creation devices in accordance with Articles 29a and 39a may be carried out without the need to obtain the qualified status for the provision of these management services until 21 May 2026.

4. Qualified trust service providers that have been granted their qualified status under this Regulation before 20 May 2024 shall submit a conformity assessment report to the supervisory body proving compliance with Article 24(1), (1a) and (1b) as soon as possible and in any event by 21 May 2026.

▼B

Article 52

Entry into force

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

2. This Regulation shall apply from 1 July 2016, except for the following:

▼B

(a) Articles 8(3), 9(5), 12(2) to (9), 17(8), 19(4), 20(4), 21(4), 22(5), 23(3), 24(5), 27(4) and (5), 28(6), 29(2), 30(3) and (4), 31(3), 32 (3), 33(2), 34(2), 37(4) and (5), 38(6), 42(2), 44(2), 45(2), and Articles 47 and 48 shall apply from 17 September 2014;

(b) Article 7, Article 8(1) and (2), Articles 9, 10, 11 and Article 12(1) shall apply from the date of application of the implementing acts referred to in Articles 8(3) and 12(8);

(c) Article 6 shall apply from three years as from the date of application of the implementing acts referred to in Articles 8(3) and 12 (8).

3. Where the notified electronic identification scheme is included in the list published by the Commission pursuant to Article 9 before the date referred to in point (c) of paragraph 2 of this Article, the recognition of the electronic identification means under that scheme pursuant to Article 6 shall take place no later than 12 months after the publication of that scheme but not before the date referred to in point (c) of paragraph 2 of this Article.

4. Notwithstanding point (c) of paragraph 2 of this Article, a Member State may decide that electronic identification means under electronic identification scheme notified pursuant to Article 9(1) by another Member State are recognised in the first Member State as from the date of application of the implementing acts referred to in Articles 8(3) and 12(8). Member States concerned shall inform the Commission. The Commission shall make this information public.

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

▼B

ANNEX I

REQUIREMENTS FOR QUALIFIED CERTIFICATES FOR ELECTRONIC SIGNATURES

Qualified certificates for electronic signatures shall contain:

(a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for electronic signature;

(b) a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least, the Member State in which that provider is established and:

— for a legal person: the name and, where applicable, registration number as stated in the official records,

— for a natural person: the person's name;

(c) at least the name of the signatory, or a pseudonym; if a pseudonym is used, it shall be clearly indicated;

(d) electronic signature validation data that corresponds to the electronic signature creation data;

(e) details of the beginning and end of the certificate's period of validity;

(f) the certificate identity code, which must be unique for the qualified trust service provider;

(g) the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;

(h) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (g) is available free of charge;

▼M2

(i) the information or the location of the services that can be used to enquire about the validity status of the qualified certificate;

▼B

(j) where the electronic signature creation data related to the electronic signature validation data is located in a qualified electronic signature creation device, an appropriate indication of this, at least in a form suitable for automated processing.

▼B

ANNEX II

REQUIREMENTS FOR QUALIFIED ELECTRONIC SIGNATURE CREATION DEVICES

1. Qualified electronic signature creation devices shall ensure, by appropriate technical and procedural means, that at least:

   (a) the confidentiality of the electronic signature creation data used for electronic signature creation is reasonably assured;

   (b) the electronic signature creation data used for electronic signature creation can practically occur only once;

   (c) the electronic signature creation data used for electronic signature creation cannot, with reasonable assurance, be derived and the electronic signature is reliably protected against forgery using currently available technology;

   (d) the electronic signature creation data used for electronic signature creation can be reliably protected by the legitimate signatory against use by others.

2. Qualified electronic signature creation devices shall not alter the data to be signed or prevent such data from being presented to the signatory prior to signing.

▼M2

_____

▼B

ANNEX III

REQUIREMENTS FOR QUALIFIED CERTIFICATES FOR ELECTRONIC SEALS

Qualified certificates for electronic seals shall contain:

(a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for electronic seal;

(b) a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least the Member State in which that provider is established and:

— for a legal person: the name and, where applicable, registration number as stated in the official records,

— for a natural person: the person's name;

(c) at least the name of the creator of the seal and, where applicable, registration number as stated in the official records;

(d) electronic seal validation data, which corresponds to the electronic seal creation data;

(e) details of the beginning and end of the certificate's period of validity;

(f) the certificate identity code, which must be unique for the qualified trust service provider;

(g) the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;

(h) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (g) is available free of charge;

▼M2

(i) the information or the location of the services that can be used to enquire about the validity status of the qualified certificate;

▼B

(j) where the electronic seal creation data related to the electronic seal validation data is located in a qualified electronic seal creation device, an appropriate indication of this, at least in a form suitable for automated processing.

▼B

ANNEX IV

REQUIREMENTS FOR QUALIFIED CERTIFICATES FOR WEBSITE AUTHENTICATION

Qualified certificates for website authentication shall contain:

(a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for website authentication;

(b) a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least the Member State in which that provider is established and:

— for a legal person: the name and, where applicable, registration number as stated in the official records,

— for a natural person: the person's name;

▼M2

(c) for natural persons: at least the name of the person to whom the certificate has been issued, or a pseudonym; if a pseudonym is used, it shall be clearly indicated;

(ca) for legal persons: a unique set of data unambiguously representing the legal person to whom the certificate is issued, with at least the name of the legal person to whom the certificate is issued and, where applicable, the registration number as stated in the official records;

▼B

(d) elements of the address, including at least city and State, of the natural or legal person to whom the certificate is issued and, where applicable, as stated in the official records;

(e) the domain name(s) operated by the natural or legal person to whom the certificate is issued;

(f) details of the beginning and end of the certificate's period of validity;

(g) the certificate identity code, which must be unique for the qualified trust service provider;

(h) the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;

(i) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (h) is available free of charge;

▼M2

(j) the information or the location of the certificate validity status services that can be used to enquire about the validity status of the qualified certificate.

▼M2

ANNEX V

REQUIREMENTS FOR QUALIFIED ELECTRONIC ATTESTATION OF ATTRIBUTES

Qualified electronic attestation of attributes shall contain:

(a) an indication, at least in a form suitable for automated processing, that the attestation has been issued as a qualified electronic attestation of attributes;

(b) a set of data unambiguously representing the qualified trust service provider issuing the qualified electronic attestation of attributes including at least, the Member State in which that provider is established and:

  (i) for a legal person: the name and, where applicable, registration number as stated in the official records;

  (ii) for a natural person: the person's name;

(c) a set of data unambiguously representing the entity to which the attested attributes refer; if a pseudonym is used, it shall be clearly indicated;

(d) the attested attribute or attributes, including, where applicable, the information necessary to identify the scope of those attributes;

(e) details of the beginning and end of the attestation's period of validity;

(f) the attestation identity code, which must be unique for the qualified trust service provider and, if applicable, the indication of the scheme of attestations that the attestation of attributes is part of;

(g) the qualified electronic signature or qualified electronic seal of the issuing qualified trust service provider;

(h) the location where the certificate supporting the qualified electronic signature or qualified electronic seal referred to in point (g) is available free of charge;

(i) the information or location of the services that can be used to enquire about the validity status of the qualified attestation..

▼M2

ANNEX VI

MINIMUM LIST OF ATTRIBUTES

Pursuant to Article 45e, Member States shall ensure that measures are taken to allow qualified trust service providers of electronic attestations of attributes to verify by electronic means at the request of the user, the authenticity of the following attributes against the relevant authentic source at national level or via designated intermediaries recognised at national level, in accordance with Union or national law and where these attributes rely on authentic sources within the public sector:

1. Address;

2. Age;

3. Gender;

4. Civil status;

5. Family composition;

6. Nationality or citizenship;

7. Educational qualifications, titles and licences;

8. Professional qualifications, titles and licences;

9. Powers and mandates to represent natural or legal persons;

10. Public permits and licences;

11. For legal persons, financial and company data.

▼M2

ANNEX VII

REQUIREMENTS FOR ELECTRONIC ATTESTATION OF ATTRIBUTES ISSUED BY OR ON BEHALF OF A PUBLIC BODY RESPONSIBLE FOR AN AUTHENTIC SOURCE

An electronic attestation of attributes issued by or on behalf of a public body responsible for an authentic source shall contain:

(a) an indication, at least in a form suitable for automated processing, that the attestation has been issued as an electronic attestation of attributes issued by or on behalf of a public body responsible for an authentic source;

(b) a set of data unambiguously representing the public body issuing the electronic attestation of attributes, including at least, the Member State in which that public body is established and its name and, where applicable, its registration number as stated in the official records;

(c) a set of data unambiguously representing the entity to which the attested attributes refer; if a pseudonym is used, it shall be clearly indicated;

(d) the attested attribute or attributes, including, where applicable, the information necessary to identify the scope of those attributes;

(e) details of the beginning and end of the attestation's period of validity;

(f) the attestation identity code, which must be unique for the issuing public body and, if applicable, an indication of the scheme of attestations that the attestation of attributes is part of;

(g) the qualified electronic signature or qualified electronic seal of the issuing body;

(h) the location where the certificate supporting the qualified electronic signature or qualified electronic seal referred to in point (g) is available free of charge;

(i) the information or location of the services that can be used to enquire about the validity status of the attestation.