2025/2532

17.12.2025

COMMISSION IMPLEMENTING REGULATION (EU) 2025/2532

of 16 December 2025

laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards reference standards and specifications for qualified electronic archiving services

THE EUROPEAN COMMISSION,

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

Having regard to Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC ([1]), and in particular Article 45j(2) thereof,

Whereas:

(1) By Regulation (EU) 2024/1183 of the European Parliament and of the Council ([2]), a list of new trust services and qualified trust services, including the qualified electronic archiving service, was introduced in Regulation (EU) No 910/2014. The Commission is to establish a list of reference standards and, where necessary, establish specifications for such services.

(2) Electronic archiving is a service for the receipt, storage, retrieval and deletion of electronic data and electronic documents to ensure their durability and legibility as well as to preserve their integrity, confidentiality and proof of origin throughout the preservation period. Qualified electronic archiving services play a crucial role in the digital business environment by promoting the transition from traditional paper-based processes to electronic equivalents. To ensure that electronic data and electronic documents preserve the presumption of their integrity and of their origin for the duration of the preservation period by the qualified trust service provider, and to achieve a high level of transparency and confidence among all participants in the information lifecycle, it is necessary to establish a common set of specifications for qualified electronic archiving services.

(3) To increase the evidentiary value, security and trustworthiness of qualified electronic archiving services, where electronic signatures, electronic seals or electronic time stamps are used to create, sign, seal or attest the date and time of, for example, archiving evidences, evidence records, records of events, records of the correct implementation of procedures, or archiving confirmation reports, qualified trust services should be used.

(4) The presumption of compliance laid down in Article 45j(2) of Regulation (EU) No 910/2014 should only apply where qualified electronic archiving services comply with the requirements set out in this Regulation. The reference standards for qualified electronic archiving services should reflect established practices and be widely recognised within the relevant sectors. They should be adapted to include additional controls ensuring the security and trustworthiness of the qualified electronic archiving services.

(5) If a trust service provider adheres to the requirements set out in this Regulation, supervisory bodies should presume compliance with the relevant requirements of Regulation (EU) No 910/2014 and duly consider such presumption for granting or confirming the qualified status of the trust service. However, a qualified trust services provider may still rely on other practices to demonstrate compliance with the requirements of Regulation (EU) No 910/2014.

(6) In order to preserve the integrity and proof of origin of electronic data and electronic documents containing one or more qualified electronic signatures or seals, qualified electronic archiving services should use procedures and technologies capable of extending the trustworthiness of those electronic signatures and seals beyond the technological validity period, at least throughout the preservation period.

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

([2]) Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework (OJ L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(7) The Commission regularly assesses new technologies, practices, standards or technical specifications. In accordance with recital 75 of Regulation (EU) 2024/1183, the Commission should review and, if necessary, update this Regulation, to keep it in line with global developments, new technologies, practices, standards or technical specifications and to follow the best practices on the internal market.

(8) Regulation (EU) 2016/679 of the European Parliament and of the Council ([3]) and, where relevant, Directive 2002/58/EC of the European Parliament and of the Council ([4]) apply to the personal data processing activities under this Regulation.

(9) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council ([5]) and delivered its opinion on 21 October 2025 ([6]).

(10) The measures provided for in this Regulation are in accordance with the opinion of the committee established by Article 48 of Regulation (EU) No 910/2014,

HAS ADOPTED THIS REGULATION:

Article 1

Electronic archiving of documents bearing a qualified electronic signature or a qualified electronic seal

1. When archiving electronic data or electronic documents that contain qualified electronic signatures or qualified electronic seals, providers of qualified electronic archiving services shall ensure that the trustworthiness of those qualified electronic signatures or qualified electronic seals is maintained, including beyond their technological validity period, and that the integrity and the accuracy of the origin of the qualified electronic signatures and seals is maintained, at least until the end of the legal or contractual preservation period.

2. For the purposes of paragraph 1, providers of qualified electronic archiving services may rely on a qualified preservation service for qualified electronic signatures or on a qualified preservation service for qualified electronic seals.

Article 2

Reference standards and specifications for the provision of qualified electronic archiving services

The reference standards and specifications referred to in Article 45j(2) of Regulation (EU) No 910/2014 are set out in the Annex to this Regulation.

([3]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([4]) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([5]) Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([6]) EDPS Formal comments on the draft Implementing Regulation laying down rules for the application of Regulation (EU) No 910/2014 as regards reference standards and specifications for qualified electronic archiving services.

Article 3

Entry into force

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

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

Done at Brussels, 16 December 2025.

For the Commission
The President
Ursula VON DER LEYEN

ANNEX

List of reference standards and specifications for qualified electronic archiving services

CEN/TS 18170:2025 ('CEN/TS 18170') applies with the following adaptations:

(a) Normative references (clause 2)

— ETSI EN 319 401 V3.1.1 (2024-06), Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers

— ETSI EN 319 421 V1.3.1 (2025-07), Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

— ISO 14721:2025, Space Data System Practices – Reference model for an open archival information system (OAIS)

— ACM-ECCG, European Cybersecurity Certification Group, Sub-group on Cryptography: 'Agreed Cryptographic Mechanisms' published by the European Union Agency for Cybersecurity ('ENISA').

— CIR (EU) 2024/482, Commission Implementing Regulation (EU) 2024/482 ([1]).

— CIR (EU) 2024/3144, Commission Implementing Regulation (EU) 2024/3144 ([2]).

— ISO/IEC 15408:2022 (parts 1 to 5), 'Information security, cybersecurity and privacy protection – Evaluation criteria for IT security'.

— FIPS PUB 140-3 (2019), "Security Requirements for Cryptographic Modules".

(b) Policy and practice statement (clause 6.1)

— The requirements of CEN/TS 18170, clause 6.1 shall apply.

— The requirements of ETSI EN 319 401, clause 5 shall apply.

— The EATSP shall establish procedures to notify the supervisory body of any changes in the provision of the electronic archiving trust service and on the intention to cease those activities, in accordance with business requirements and relevant laws and regulations, including in accordance with the requirements of the implementing acts adopted pursuant to Article 24(5) of Regulation (EU) No 910/2014 [i.2].

— The EATSP shall notify the competent supervisory body at least:

  — one month before implementing any change;

  — three months before the planned cessation of a trust service provision.

(c) Terms and Conditions (clause 6.2)

— The requirements of CEN/TS 18170, clause 6.2 shall apply.

— Subscribers and parties relying on the electronic archiving trust service shall be informed, in a clear, comprehensive and easily accessible manner, in a publicly accessible space and individually, of precise terms and conditions, before entering into a contractual relationship.

([1]) Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC) (OJ L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

([2]) Commission Implementing Regulation (EU) 2024/3144 of 18 December 2024 amending Implementing Regulation (EU) 2024/482 as regards applicable international standards and correcting that Implementing Regulation (OJ L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj).

(d) Human resources (clause 7.3)

— The requirements of CEN/TS 18170, clause 7.3 shall apply.

— EATSP's personnel in trusted roles, and if applicable its subcontractors in trusted roles, shall be able to fulfil the requirement of 'expert knowledge, experience and qualifications' through formal training and credentials, or actual experience, or a combination of the two. This shall include regular updates (at least every 12 months) on new threats and current security practices.

(e) Cryptographic controls and monitoring (clause 7.6)

— The archiving system must guarantee the confidentiality of data and documents through the lifecycle of the archive from its deposit to its elimination.

— The requirements specified in ETSI EN 319 401, sub-clause 7.5 "Cryptographic controls" shall apply.

— The origin of the data to be archived in the electronic archiving system shall be established by the EATSP If they use electronic signatures or electronic seals to do so, those electronic signatures or electronic seals shall be qualified.

— When EATSP digitally signs (part of) a digital object or record, the EATSP private signing key shall be held and used within either a qualified electronic signature or seal creation device or a secure cryptographic device which is a trustworthy system certified in accordance with:

(a) Common Criteria for Information Technology Security Evaluation, as set out in ISO/IEC 15408 or in Common Criteria for Information Technology Security Evaluation, version CC:2022, Parts 1 through 5, published by the participants of the Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security, and certified to EAL 4 or higher; or

(b) the European Common Criteria-based cybersecurity certification scheme (CIR (EU) 2024/482, CIR (EU) 2024/3144) and certified to EAL 4 or higher; or

(c) until 31.12.2030, FIPS PUB 140-3 level 3.

— This certification shall be to a security target or protection profile, or to a module design and security documentation, which meets the requirements of the present document, based on a risk analysis and taking into account physical and other non-technical security measures.

— If the secure cryptographic device benefits from an EUCC certification (IR (EU) 2024/482, CIR (EU) 2024/3144), then this device shall be configured and used in accordance with that certification.

— The EATSP shall monitor the strength of cryptographic algorithm that was and are used. In case, one of the used algorithms or parameters is thought to become not suitable as defined in the risk management, the EATSP shall either update the related archiving policy or create a new archiving profile to handle the AIPs and define and perform appropriate measures.

— The evaluation of the cryptographic algorithms and their use by the EATSP shall be compliant with the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group and published by ENISA (ACM-ECCG).

— Technical components of the EATS shall authenticate each other based on cryptographic techniques before communicating.

(f) Network (clause 7.9)

— The requirements specified in ETSI EN 319 401, sub-clause 7.8 "Network security" shall apply.

— The vulnerability scan requested by REQ-7.8-13 of ETSI EN 319 401 shall be performed at least once per quarter.

— The penetration test requested by REQ-7.8-17X of ETSI EN 319 401 shall be performed at least once per year.

— Firewalls shall be configured to prevent all protocols and accesses not required for the operation of the EATSP.

(g) Collection of evidence (clause 7.11)

— The requirements specified in ETSI EN 319 401, sub-clause 7.10 “Collection of evidence” shall apply, including for critical and non-critical events (see subclause 13.2)

(h) EATSP termination and termination plan (clause 7.13)

— The requirements of CEN/TS 18170, clause 7.13) shall apply.

— The EATSP’s termination plan shall comply with the requirements set out in the implementing acts adopted pursuant to Article 24(5) of Regulation (EU) No 910/2014.

(i) Reliable time of events (clause 13.3.1)

— The requirements of CEN/TS 18170, clause 13.3.1) shall apply.

— When using timestamps the EATSP shall use a qualified timestamp.