Official Journal
of the European Union

EN
L series

2025/2160

28.10.2025

COMMISSION IMPLEMENTING REGULATION (EU) 2025/2160

of 27 October 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, specifications and procedures for the management of risks to the provision of non-qualified trust 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 19a(2) thereof,

Whereas:

(1) Non-qualified trust service providers play an important role in the digital environment by providing trust services that facilitate secure electronic transactions. Regulation (EU) No 910/2014 places fewer regulatory requirements on non-qualified trust service providers than on qualified trust service providers. However, all trust service providers are subject to requirements on security and liability to ensure due diligence, transparency and accountability of their operations and services.

(2) Non-qualified trust service providers can be considered important or essential entities in accordance with Article 3 of Directive (EU) 2022/2555 of the European Parliament and of the Council ([2]). Thus, Commission Implementing Regulation (EU) 2024/2690 ([3]) laying down technical and methodological requirements of cybersecurity risk management measures applies to them. However, the scope of the requirements laid down in Article 19a(1), point (a), of Regulation (EU) No 910/2014 relates to the risk management procedures concerning legal, business, operational and other direct or indirect risks to the provision of non-qualified trust services. To complement the risk management framework set out in Implementing Regulation (EU) 2024/2690 and to enable a coherent approach to the management of all relevant types of risks, specifications and procedures concerning the management of those risks by non-qualified trust service providers should be laid down. Guidance provided by the European Union Agency for Cybersecurity (ENISA) or national competent authorities under Directive (EU) 2022/2555 can support non-qualified trust service providers in the design and implementation of appropriate risk management policies.

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

([2]) Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on 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, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

([3]) Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers (OJ L, 2024/2690, 18.10.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2690/oj).

(3) The presumption of compliance laid down in Article 19a(2) of Regulation (EU) No 910/2014 should only apply where non-qualified trust service providers comply with the requirements set out in this Regulation. The reference standards referred to in the Annex should reflect established practices and be widely recognised within the relevant sectors. In order to ensure that non-qualified trust service providers manage legal, business, operational and other direct or indirect risks to the provision of the non-qualified trust service in accordance with Article 19a(1) of Regulation (EU) No 910/2014, non-qualified trust services providers should comply with the referenced elements of the standards as set out in the Annex and with the risk management requirements set out in this Regulation for the presumption of compliance.

(4) If a non-qualified trust service provider adheres to the requirements set out in this Implementing Regulation, supervisory bodies should presume compliance with the relevant requirements of Regulation (EU) No 910/2014. However, a non-qualified trust services provider may still rely on other practices to demonstrate compliance with the requirements of the Regulation (EU) No 910/2014.

(5) To ensure that the identified risks are adequately addressed, the risk management policies followed by non-qualified trust service providers should include procedures for risk documentation and evaluation, as well as for the identification, selection and implementation of appropriate risk treatment measures. The implementation of risk treatment measures should be continuously monitored. As regards the information that non-qualified trust service providers record and retain as part of their risk treatment measures, non-qualified trust service providers should ensure the integrity and confidentiality of such data. Moreover, to enhance transparency and to support supervisory activities, non-qualified trust service providers should publish the identity verification methods they apply. As not all identified risks may be fully addressed through their avoidance, mitigation or transfer to other entities, any residual risks should be approved by the management bodies of non-qualified trust service providers. Criteria for the acceptance of residual risks should be justified in a comprehensible manner.

(6) The Commission regularly assesses new technologies, practices, standards or technical specifications. In accordance with Recital 75 of Regulation (EU) 2024/1183 of the European Parliament and of the Council ([4]), the Commission should review and, if necessary, update this Implementing 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.

(7) Regulation (EU) 2016/679 of the European Parliament and of the Council ([5]) and, where relevant, Directive 2002/58/EC of the European Parliament and of the Council ([6]) apply to the personal data processing activities under this Regulation.

(8) 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 ([7]) and delivered its opinion on 8 August 2025 ([8]).

([4]) 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).

([5]) 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).

([6]) 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).

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

([8]) EDPS Formal comments on the draft Implementing Regulation as regards specifications and procedures for the management of risks to the provision of non-qualified trust services | European Data Protection Supervisor.

(9) 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

Reference standards

The reference standards referred to in Article 19a(2) of Regulation (EU) No 910/2014 are set out in the Annex to this Regulation.

Article 2

Risk management policies

1. The risk management policies referred to in Article 19a(1) of Regulation (EU) No 910/2014 shall clearly identify the trust services they apply to, shall be specific to the trust services concerned and shall be approved by the management body of the non-qualified trust service provider.

2. The risk management policies shall include at least all the following elements:

(a) the overall risk tolerance level in accordance with the criticality and required level of security of the trust services, having regard to the latest technological developments;

(b) the relevant risk criteria, including at least the likelihood, impact and level of the risk, taking into account cyber threat intelligence and vulnerabilities;

(c) an approach for the identification and documentation of the risks to the provision of the trust services, taking into account the complete scope of the information system used by the non-qualified trust service provider, including risks associated with the components of the system as well as with any active or passive parties involved in the implementation of the system or in the provision of the trust services;

(d) a process for the evaluation of the identified risks based on the risk criteria referred to in point (b);

(e) a process for the identification, prioritisation and continuous monitoring of the implementation of appropriate risk treatment measures;

(f) a process for continuous monitoring of the implementation of the risk management policies.

3. Non-qualified trust service providers shall establish appropriate procedures and maintain documents to ensure that the requirements set out in the applicable legislation are implemented.

4. Non-qualified trust service providers shall establish appropriate documented procedures ensuring the monitoring of Union and national legislative and regulatory changes that may impact the provision of trust services.

Article 3

Identification, documentation and evaluation of risks

Non-qualified trust service providers shall identify, document and evaluate all risks referred to in Article 19a(1) of Regulation (EU) No 910/2014 in accordance with the risk management policies referred to in Article 2, and shall in particular:

(a) identify risks in relation to third parties;

(b) identify potential single point of failure in the provision of the trust services;

(c) evaluate the identified risks based on the risk criteria referred to in Article 2(2), point (b).

Article 4

Risk treatment measures

1. In accordance with the policies referred to in Article 2, non-qualified trust service providers shall plan, document and implement risk treatment measures, and shall, in particular, carry out the following tasks:

(a) identify and prioritise appropriate risk treatment measures;

(b) select, approve and document the chosen risk treatment measures, including their security requirements and operational procedures, in a risk treatment plan, identify who is responsible for implementing the risk treatment measures and when they are to be implemented;

(c) continuously monitor the implementation of the risk treatment measures.

2. The risk treatment plan set out in paragraph 1, point (b), shall provide reasons justifying the acceptance of residual risks in a comprehensible manner.

3. As part of the risk treatment measures referred to in paragraph 1, non-qualified trust service providers shall also:

(a) verify, where applicable, the identity of the users of the trust service directly or by means of a third party and publish information on the identity verification methods used;

(b) for the purposes of providing evidence in legal proceedings and of ensuring service continuity, record and securely retain for as long as necessary in accordance with Union or national laws, including after the activities of the non-qualified trust service provider have ceased, the following information:

— all relevant information collected in the process of registration and onboarding of the trust service users, including, where applicable, the identity verification of the users,

— authentication data assigned to the user of the trust service, where applicable, and

— any change of the status of public key certificates or other cryptographic material used in the provision of the trust service.

(c) ensure, where applicable, that authentication data assigned to the user of the trust service are unique.

4. When identifying, selecting, approving and prioritising appropriate risk treatment measures, non-qualified trust service providers shall take into account the following elements:

(a) the results of the risk evaluation referred to in Article 3;

(b) the effectiveness of the risk treatment measures;

(c) conformity assessments;

(d) significant incidents;

(e) the cost of implementation in relation to the expected benefit;

(f) the applicable appropriate asset classification;

(g) the analysis of any business impact of the risks identified in accordance with Article 3.

5. The management bodies of non-qualified trust service providers shall approve the residual risks remaining after the implementation of the risk treatment measures as set out in the risk treatment plan.

6. Non-qualified trust service providers shall review, document and, where appropriate, update the risk evaluation results and the risk treatment plan at planned intervals, and at least annually, and when significant changes to the infrastructure, operations or risks, or significant incidents, occur.

7. Non-qualified trust service providers shall ensure the availability, integrity and confidentiality of the information referred to in paragraph 3, point (b).

Article 5

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, 27 October 2025.

For the Commission
The President
Ursula VON DER LEYEN

ANNEX

List of reference standards for non-qualified trust service providers

Requirements under the following clauses of the standard ETSI EN 319 401 V3.1.1 (2024-06): 'Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers' shall apply:

5. Risk Assessment;
6. Policies and practices;
7.1 Internal organization;
7.2 Human resources;
7.3 Asset management;
7.4 Access control;
7.6 Physical and environmental security.