Order approving the procedure for granting, suspending and withdrawing the status of a qualified trust service provider,
the procedure for registration and deregistration of non-qualified trust service providers in the Register of non-qualified trust service providers,
the procedure for registration and deregistration of non-qualified trust service providers in the field of defence, public order and national security in the Register of non-qualified trust service providers,
the procedure for supervision, inspection and sanctioning of trust service providers and approval of the rules for the approval of validation mechanisms

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, as subsequently amended and supplemented;
- Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market;
- Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market;
- Commission Implementing Decision (EU) No 2015/296 of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to Article 12(7) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market;
- Commission Implementing Decision (EU) No 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic

identification and trust services for electronic transactions in the internal market;

- Commission Implementing Decision (EU) No 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market;
- Commission Implementing Decision (EU) 2015/1984 of 3 November 2015 defining the circumstances, formats and procedures for notification, pursuant to Article 9(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market;
- Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market;
- Law No 214/2024 on the use of electronic signatures, timestamps and the provision of trust services based on them;
- Decision No 89/2020 on the organisation and functioning of the Authority for the Digitalisation of Romania, as subsequently amended and supplemented;

Pursuant to the provisions of Article 10(4) of Law No 214/2024 on the use of electronic signatures, timestamps and the provision of trust services based on them and Article 12(3) of Decision No 189/2025 on the organisation and functioning of the Ministry of the Economy, Digitalisation, Entrepreneurship and Tourism, the Minister for the Economy, Digitalisation, Entrepreneurship and Tourism hereby issues this

ORDER

Article 1. The procedure for granting, suspending and withdrawing the status of a qualified trust service provider, as set out in Annex 1, is hereby approved.

Article 2. The procedure for the registration and deregistration of non-qualified trust service providers in the Register of non-qualified trust service providers, as set out in Annex 2, is

hereby approved.

Article 3. The procedure for the registration and deregistration of non-qualified trust service providers in the field of defence, public order and national security in the Register of non-qualified trust service providers, as set out in Annex 3, is hereby approved.

Article 4. The procedure for supervision, inspection and sanctioning of trust service providers, as set out in Annex 4, is hereby approved.

Article 5. The Rules for the approval of validation mechanisms, set out in Annex 5, are hereby approved.

Article 6. - (1) This Order will enter into force 90 days after its publication in the Official Gazette.

(2) Trust service providers providing trust services on the date of publication of this Order in the Official Gazette of Romania (*Monitorul Oficial al României*), Part I, are required to submit updated documentation to the Authority for the Digitalisation of Romania in accordance with the present procedures provided for in Article 1(2) within 270 days of their entry into force or by the expiry date of the current accreditation, whichever is the sooner.

Article 7. On the date of entry into force of this Order, Order No 449/2017 of the Minister for Communications and Information Society on the procedure for granting, suspending and withdrawing the status of a qualified trust service provider in accordance with Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 is repealed.

Article 8. Annexes Nos 1–5 form an integral part of this Order.

Minister

Annex 1

PROCEDURE

for granting, suspending and withdrawing the status of a qualified trust service provider

CHAPTER I Purpose, subject matter, scope and legal framework of the procedure

Article 1. This procedure establishes the operational, institutional and technical framework for granting, suspending and withdrawing the status of a qualified trust service provider, in accordance with the provisions of Law No 214/2024 on the use of electronic signatures, timestamps and the provision of trust services based on them and of 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, as subsequently amended and supplemented.

Article 2. The procedure applies to all legal entities applying to be granted the status of a qualified trust service provider, as well as to those in possession of that status and subject to assessment, supervision and, where applicable, suspension or withdrawal measures.

Article 3. The legal framework of the procedure is represented by:

a) 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, as subsequently amended and supplemented, hereinafter referred to as Regulation (EU) No 910/2014;
b) Law No 214/2024 on the use of electronic signatures, timestamps and the provision of trust services based on them, hereinafter referred to as Law No 214/2024;
c) Government Decision No 189/2025 on the organisation and functioning of the Ministry of the Economy, Digitalisation, Entrepreneurship and Tourism;
d) Government Decision No 89/2020 on the organisation and functioning of the Authority for the Digitalisation of Romania, as subsequently amended and supplemented.

CHAPTER II Powers of the Authority for the Digitalisation of Romania

Article 4. In fulfilling the role provided for in Article 19 of Law No 214/2024, the Authority for the Digitalisation of Romania, hereinafter referred to as the ADR, as the supervisory body and regulatory and supervisory authority specialised in the field:

(1) grants, suspends or withdraws the status of qualified trust service provider;

(2) ensures that qualified trust service providers established on Romanian territory and the qualified trust services they provide meet the requirements laid down in Regulation (EU) No 910/2014 and Law No 214/2024;

(3) calls on trust service providers to remedy any failure to comply with the requirements provided for in Regulation (EU) No 910/2014, as subsequently amended and supplemented, and in Law No 214/2024.

CHAPTER III Submission of the notification and documentation

Article 5. - (1) Legal persons intending to provide qualified trust services, including those intending to provide trust services within closed systems, shall submit notification of their intention to the regulatory and supervisory authority specialised in the field, according to the template set out in Annex 1.1 to this procedure, 30 days before the start of their activity, in order to be registered in the Register of qualified trust service providers.

(2) The notification provided for in paragraph (1) must be accompanied by the following documents:

a) a conformity assessment report, issued by a conformity assessment body, which will include the minimum information provided for in Annex 1.2 to this procedure, as well as all information relating to the security and certification procedures used;
b) a letter of guarantee from a financial-banking institution, or a civil liability insurance policy for the risks associated with the provision of each trust service for which qualified status is requested, to the amount of EUR 500 000 for each trust service, assigned to the supervisory body;
c) a description of the technical solution;
d) the self-declaration of the provider’s legal representative regarding compliance, in the context of the process of providing trust services, with the requirements of 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);

e) the security plan of the information system used;
f) links to the policies, practices and procedures for providing qualified trust services;
g) the detailed architecture of the trust service (e.g. the public key infrastructure [PKI] hierarchy, together with an indication of the supported trust service policies) for which qualified status is requested;
h) the terms and conditions that the qualified trust service provider will sign with the end user;
i) the contact details of the trust service provider (email, telephone number, website);
j) the memorandum of association of the trust service provider showing that it has specified in its scope of activity that it carries out activities in the fields of information technology or information services;
k) power of attorney for the person delegated to sign on behalf of the administrator;
l) evidence that the trust service provider has sufficient financial resources and has obtained adequate liability insurance in respect of provision of the trust services for which a qualified status is requested, including copies of the profit and loss account and the accounting balance for the last 3 years for accounts that were registered; failing this, appropriate bank statements;
m) business continuity and disaster recovery plan;
n) the list of standards on the basis of which operations are carried out, audited, assessed or certified compliant;
o) certificate of conformity for electronic signature and electronic seal creation devices in accordance with the requirements of Regulation (EU) No 910/2014, as subsequently amended and supplemented, and Commission Implementing Decision (EU) No 650/2016;
p) presentation of the technical and organisational measures taken to manage the risks posed to the security of trust services, intended to support demonstration of the requirement of Article 19(1) of Regulation (EU) No 910/2014;
q) the procedure for notifying the personal data supervision and protection authority of a security breach or loss of integrity that has a significant impact on the trust service provided or on the personal data retained by the service provider intended to support demonstration of the requirement of Article 19(2) of Regulation (EU) No 910/2014, as subsequently amended and supplemented;
r) the activity cessation plan in accordance with the requirements of Article 24(2). (i) of Regulation (EU) No 910/2014, as subsequently amended and supplemented;
s) the provider’s WEB address;
t) the order of accreditation as an electronic archive administrator, in accordance with the provisions of Law No 135/2007 on the archiving of electronic documents, or the contract concluded with an accredited electronic archive administrator;
u) minimum one precise source of time, linked to universal time, in compliance with the business continuity and disaster recovery requirements.

(3) All documents must be signed by the legal manager or authorised person, electronically using a qualified certificate, or handwritten, and transmitted to the ADR in original.

Article 6. The ADR shall review the notification and documentation within a maximum of 30 days. If all legal conditions are met, the provider is registered in the Trusted List and the decision granting qualified trust service provider status is issued.

CHAPTER IV Periodic assessment and ongoing supervision

Article 7. - (1) Qualified providers shall be assessed by a conformity assessment body, at their own expense and at least every 24 months, regarding their fulfilment of the requirements laid down in Regulation (EU) No 910/2014 and Law No 214/2024.

(2) the assessment report shall be sent to the ADR within 3 working days of its receipt.

Article 8. (1) Qualified trust service providers shall inform the supervisory body at least 30 days before the start of the conformity assessment activity and, upon request, allow the supervisory body to participate as an observer.

(2) Qualified trust service providers are obliged to retain the information used for and regarding the traceability of the activity of issuing qualified certificates for a period of 10 years and to take measures for the long-term preservation (LTP) of the trust chain so that the electronic signatures of digital certificates in the trust chain remain valid, authentic and legally admissible in the long term.

CHAPTER V Suspension and withdrawal of qualified status

Article 9. -(1) The ADR, as the supervisory body, shall inform the qualified trust service provider of the suspension or withdrawal of its qualified status. The supervisory body shall inform the body notified under Article 22(3) of Regulation (EU) No 910/2014, for the purpose of updating the trusted lists referred to in paragraph (1) of that Article, as well as the competent authority designated or established under Article 8(1) of Directive (EU) 2022/2555.

(2) Should a trust service provider that issues qualified digital certificates cease its activity, the specialised regulatory and supervisory authority in the field shall ensure either that certificates issued by the trust service provider are revoked or that the activity and the electronic register of

certificates issued and revoked are taken over by another trust service provider, with its consent. Any of these measures shall be communicated to the certificate holders immediately.

(3) If the activity of the trust service provider is not taken over by another provider, the trust service provider is obliged to ensure the revocation of all certificates it has issued. Should it fail to do so, they will be revoked by the ADR at the provider’s expense.

ANNEX 1.1 to the procedure

Notification template

with a view to obtaining the status of qualified trust service provider

Dear Mr/Ms President,

The undersigned [*name of applicant legal person*], whose registered office is at [*full address*], registered with the Trade Register Office under No [*J/…/…*], with unique tax registration number [*CUI/CIF*], legally represented by [*Personal name and surname*], identified by [*identification document series, number, personal identification number*], pursuant to the provisions of Article 19 and Article 21 of Law No 214/2024 and Regulation (EU) No 910/2014, hereby submit to you this notification of intention to obtain the status of qualified trust service provider for the following trust service:

[*name of the service for which qualified status is requested*].

We request that you launch the procedure to review the attached documentation with a view to our registration in the Register of Qualified Trust Service Providers and inclusion in the Trusted List.

Applicant contact details:

email: _____

Telephone: _____

Website: _____

Signature of legal representative:

[handwritten or qualified electronic signature]

Date: _____

Annex: List of the supporting documents provided for in Article 5(2) of the procedure (listed in full, in alphabetical order a–u/v, signed and dated).

ANNEX 1.2 to the procedure

Minimum compulsory information included in the conformity assessment report

The conformity assessment report must include the following elements:

1. Clearly indicate the name of the conformity assessment body and, where applicable, its registration number as stated in the official records, its official postal address and its electronic mail address.
2. Clearly indicate the name of the nationally recognised accreditation body in the Member State that granted the conformity assessment body its accreditation and, where applicable, the registration number of the national accreditation body as stated in the official records, its official postal address and electronic mail address.
3. Include the accreditation certificate or a link to the location at which the accreditation certificate issued by the national accreditation body identified under point 2 can be accessed, together with the detailed description, or a link to the location at which a detailed description of the accreditation scheme can be obtained, including an indication of its relevance in relation to Regulation (EU) No 910/2014, as amended.
4. Clearly indicate the name of the lead auditor or conformity assessment body having issued and signed the conformity assessment report.
5. The audit opinion as to whether or not the provider complies with the requirements of Regulation (EU) No 910/2014, as amended, for the trust service for which it has been audited.
6. The trust service for which the trust service provider has been assessed.
7. The standard(s) in accordance with which the conformity assessment was carried out.
8. Clearly indicate which of the trust provider's services the conformity assessment report certifies compliant with the requirements of Regulation (EU) No 910/2014, as subsequently amended and supplemented. Identification of the service(s) will be aligned with Commission Implementing Decision (EU) 2015/1505 and clause 5.5.1.1 of ETSI TS 119 612 V2.1.1 or latest version (note: in this regard, it must include at least the Subject Key Identifier RFC 5280 or the public key of the audited trust services and the Base64 PEM representation of the associated X.509 v3 digital certificate).
9. Provide for each qualified trust service identified under point 8 such information as is necessary to enable the service(s) to be identified for inclusion in the applicable national trusted list, in accordance with Commission Implementing Decision (EU) 2015/1505 of 8 September 2015.
10. Provide a complete list of the public documents and internal documents of the trust service provider that were included in the scope of the audit.

The public documents that must be attached to the conformity assessment report or be provided with publicly accessible links enabling the documents to be downloaded.

a) The public documents included in the scope of the conformity assessment shall include at least:

   (i) the declaration of the practices used by the trust service provider to provide qualified trust services;

   (ii) the qualified trust service policy/ies, for example the set of rules indicating the applicability of qualified trust services to a specific community and/or applications with common security requirements;

   (iii) the terms and conditions of the contract for the provision of trust services.

b) The internal documents included in the scope of the audit shall include at least:

   (i) the service termination plan referred to in Article 24(2). (i) of Regulation (EU) No 910/2014 as subsequently amended and supplemented;

   (ii) the documentation relating to the risk assessment intended to support demonstration of the requirement of Article 19(1) of Regulation (EU) No 910/2014, as subsequently amended and supplemented;

   (iii) the procedure for notifying a security breach or loss of integrity that has a significant impact on the trust service provided or on the personal data retained by the service provider intended to support demonstration of the requirement of Article 19.2 of Regulation (EU) No 910/2014 as subsequently amended and supplemented;

   (iv) a list of all internal documents supporting the trust service provider's declaration of practices used to provide qualified trust services and the policy(s) of the qualified trust services.

11. Indicate, for each stage of the audit (e.g. documentation audit and implementation audit, including on-site inspections), the period during which the audit was carried out (the time elapsed) and the human-day effort expended by the conformity assessment body to perform the audit.

12. Meet the requirements laid down by the standards in force.

A. General requirements for qualified trust service providers and for each type of qualified trust service [indicating the relevant articles of Regulation (EU) No 910/2014, as subsequently amended and supplemented].

B. Additional specific requirements for the applicable type of qualified trust service [indicating the relevant articles of Regulation (EU) No 910/2014, as subsequently amended and supplemented].

1. The audit report issued on the basis of standards or on the basis of publicly available specifications shall separately highlight points of non-compliance and their impact on qualified trust services provided by the trust service provider.
2. Detail the list of third parties contracted by the trust service provider to perform all or parts of the underlying processes for the provision of its qualified trust services (e.g. Internet service providers, courier services, infrastructure, etc.). The conformity assessment report shall specify which of these parties have been audited.
3. Indicate, when requested by the applicable accreditation/conformity assessment scheme, when the next supervision audit and conformity audit should be performed.
4. Indicate the circumstances under which an accredited conformity assessment body should be brought in to reassess the trust service provider and qualified trust services, in addition to the planned audits.
5. Auditor conflict of interest declaration.

Annex 2

PROCEDURE

for the registration and deregistration of non-qualified trust service providers in the Register of non-qualified trust service providers

CHAPTER I Purpose, subject matter, scope and legal framework of the procedure

Article 1. This procedure regulates the institutional and technical framework for the registration and deregistration of non-qualified trust service providers in the Register provided for in Article 21 of Law No 214/2024 on the use of electronic signatures, timestamps and the provision of trust services based on them.

Article 2. The procedure applies to all legal persons intending to provide non-qualified trust services, as well as to those that already carry out these activities and are subject to the supervisory regime established by law.

Article 3. The applicable legal framework is as follows:

a) 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, as subsequently amended and supplemented, hereinafter referred to as Regulation (EU) No 910/2014;
b) Law No 214/2024 on the use of electronic signatures, timestamps and the provision of trust services based on them, hereinafter referred to as Law No 214/2024;
c) Government Decision No 189/2025 on the organisation and functioning of the Ministry of the Economy, Digitalisation, Entrepreneurship and Tourism;
d) Government Decision No 89/2020 on the organisation and functioning of the Authority for the Digitalisation of Romania, as subsequently amended and supplemented.

CHAPTER II Powers of the Authority for the Digitalisation of Romania

Article 4. Pursuant to Article 21 of Law No 214/2024, the Authority for the Digitalisation of Romania (ADR):

a) maintains the Register of non-qualified trust service providers;
b) analyses registration applications and the associated documentation;

c) orders registration or deregistration, as appropriate;
d) checks providers' compliance with the applicable legal requirements;
e) asks service providers to implement remedial measures where non-conformities are identified.

CHAPTER III Registration procedure

Article 5. - (1) Legal persons intending to provide unqualified trust services shall submit an application to the ADR at least 30 days before the start of the activity, using the template provided in Annex 2.1, accompanied by the documentation provided for in paragraph (2).

(2) The documentation shall be submitted electronically, signed with a qualified electronic signature by the legal representative or the person empowered to do so, or sent as a letter with a handwritten signature, and shall include, cumulatively, the following documents:

a) An audit report, issued by an auditor listed on the DNSC (National Cybersecurity Directorate) List of Validly Certified Cybersecurity Auditors (LASC), holding a General certificate, managed and published on the DNSC website and complying with the requirements of ETSI EN 319 403-1 V2.3.1 (2020-06) – 'Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers', or subsequent versions, including the following activities:
    i. Architectural audit – consists in checking the compliance of the security measures relating to the choice, positioning and implementation of hardware/software devices in computer networks and systems, minimum security requirements and the internal policies of the economic operator. The audit may be extended to interconnections with third-party networks, including the Internet.
    ii. Configuration audit – this consists in checking the implementation of security measures according to the state of the art, the minimum security requirements and the security policies as regards the configuration of hardware/software devices comprising network and information systems. These devices may particularly include network equipment, operating systems (server or workstation), applications or security products.
    iii. Penetration audit or penetration testing consists in identifying vulnerabilities in network and information systems and checking how they might be exploited as well as the impact of their exploitation on the network, under the real conditions of a cyber-attack on network and information systems. Auditing may be performed either from outside the

network (particularly from the Internet or an interconnected network of a third party) or from within the network and should be performed in complementarity with other auditing activities in order to improve their effectiveness or to demonstrate the feasibility of exploiting the vulnerabilities discovered.

iv. Organisation security audit – consists of an audit of the organisation's logical and physical security and aims to ensure that the security policies and procedures defined by the economic operator are in line with the security needs of the audited economic operator, the level of technology and the standards in force, that they correctly complement the technical measures implemented and are effectively implemented.

v. Information regarding the security and certification procedures used.

vi. Ensuring that qualified trust service providers established on Romanian territory and the qualified trust services they provide meet the requirements laid down in Regulation (EU) No 910/2014 and Law No 214/2024, as subsequently amended and supplemented, and Law No 214/2024 and, in this regard, the audit report must show compliance with at least the following:

(i) in the case of service providers issuing certificates for advanced electronic signature, ETSI Standard EN 319 411-1 V1.4.1 (2023-10) ESI Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements, or subsequent versions, and the conditions specified in Article 26(1) of Regulation (EU) No 910/2014, as subsequently amended and supplemented;

(ii) in the case of trust service providers issuing advanced signature tools other than digital certificates, ETSI Standard EN 319 401 V2.3.1 (2021-05) – Electronic Signatures and Infrastructures (ESI), General Policy Requirements for Trust Service Providers, or later versions, and the conditions specified in Article 26(1) of Regulation (EU) No 910/2014, as subsequently amended and supplemented;

(iii) ETSI TS 119 461 V2.1.1 (2025-02) – ESI; Policy and security requirements for trust service components providing identity proofing of trust service subjects, or subsequent versions, for Baseline LoIP minimum level.

b) A letter of guarantee from a financial-banking institution or a liability insurance policy for risks associated with the provision of trust services, for the amount of EUR 100 000.

c) A description of the technical solution;
d) The self-declaration of the provider's legal representative regarding compliance, in the context of the process of providing trust services, with the requirements of 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).
e) The security plan of the information system used.
f) The policies, and procedures for providing trust services.
g) The detailed architecture of the trust service (e.g. PKI – public key infrastructure hierarchy).
h) A self-declaration from the legal representative stating that staff with specialised knowledge, experience and qualifications are involved in the process of issuing trust services, as well as the training plan in accordance with the provisions of Article 12(2) (e) of Law No 214/2024.
i) The terms and conditions communicated by the trust service provider and accepted by the end user, when issuing advanced signatures with a certificate, as well as the detailed description of the advanced signature validation mechanism, when its approval by the ADR has not been requested, through the procedure described in Annex 5.
j) The contact details of the trust service provider (email, telephone number, website).
k) The memorandum of association of the trust service provider showing that it has specified in its scope of activity that it carries out activities in the fields of information technology or information services, except where the trust services relate to the activities that it is authorised to carry out, in which case it must prove that it holds possession of the CAEN code corresponding to the activity carried out in the fields of information technology or information services.
l) Power of attorney for the person delegated to sign on behalf of the legal representative of the trust service provider.
m) Evidence that the trust service provider has sufficient financial resources and has obtained adequate liability insurance in respect of provision of the trust services for which a status qualified as requested, including copies of the profit and loss account and the accounting balance for the last 3 years for accounts that were registered; failing this, appropriate bank statements, or in the event that the trust service provider is a newly established legal person, must show evidence that it holds social capital to the tune of RON 10 000.
n) Business continuity and disaster recovery plan.
o) The list of standards on the basis of which operations are carried out, audited, assessed or certified compliant.

p) The procedure for notifying the National Personal Data Processing Supervisory Authority of a security breach or loss of integrity that has a significant impact on the trust service provided or on the personal data retained by the service provider intended to support demonstration of the requirement of Article 19(2) of Regulation (EU) No 910/2014, as subsequently amended and supplemented.
q) Certificates of conformity of the devices used to issue certificates for advanced electronic signature.
r) The plan for cessation of activity.
s) The provider's web address.
t) The decision regarding accreditation as an electronic archive administrator, in accordance with the provisions of Law No 135/2007 on the archiving of electronic documents, or the contract concluded with an accredited electronic archive administrator.
u) The employment scheme of the staff involved in the process of issuing trust services, their certification/qualifications and the training plan in accordance with Article 12(2) (e) of Law No 214/2024 on the use of electronic signatures, timestamps and the provision of trust services based on them.
v) Minimum one precise source of time, linked to universal time, in compliance with the business continuity and disaster recovery requirements.

Article 6. Trust service providers issuing advanced electronic signature certificates shall be obliged to use, in the identification process of the certificate applicant, identification means regulated and recognised at national level, including, where available, electronic identification means and relevant trust services provided for by:

a) Regulation (EU) No 910/2014, as subsequently amended and supplemented;
b) Law No 214/2024 on the use of electronic signatures, timestamps and the provision of trust services based on them;
c) any other secure, remote or electronic identification process that is regulated, recognised, approved or accepted at national level by the Authority for the Digitalisation of Romania.

Article 7. The ADR shall review the application and documentation within 30 days of the date of receipt. The technical advice shall be granted taking into account the regulatory technical specifications/implementing technical standards (RTS/ITS), issued pursuant to the Regulation and made available by the National Qualifications Authority (ANC), as well as validation of the cybersecurity report by the DNSC. If the legal conditions are met, the provider is registered in the Register of non-qualified trust service providers and the Decision granting the status of a non-qualified trust service provider is issued.

Article 8. - (1) In order to remain in the Register, providers are obliged to carry out, at their own expense, a full audit of the information system every two years at most, using an external auditor included in the DNSC list and holding a General Certificate. Where the provider has been involved in a cybersecurity incident that caused damage, the time limit for completing the audit shall be reduced to 1 year from the date of the incident.

(2) the same cybersecurity audit service provider may not be used for more than two consecutive audits.

(3) in the event of significant changes in the technical, administrative, functional or security architecture of the IT system used to provide non-qualified electronic signature services – such as replacement or reconfiguration of signature engines, cryptographic modules, authentication mechanisms, processing streams or critical interfaces – the provider is required to notify ADR at least 10 calendar days prior to implementation of the change and to request a new cybersecurity audit, prior to resuming or continuing to provide the service.

(2) the audit report shall be sent to the ADR within 3 working days of its finalisation.

(3) public institutions issuing digital certificates for advanced signatures are obliged to submit the same documentation provided for in Article 5(2).

Article 9. Providers are required to notify the ADR at least 30 days before the start of any audit, and the ADR may appoint representatives to participate as observers.

Article 10. Any changes to the data or documents submitted for registration must be communicated to ADR within a maximum of 60 days, together with proof that they have been updated.

CHAPTER IV Deregistration from the Register

Article 11. (1) Deregistration from the Register shall be ordered in the following cases:

a) at the request of the provider;
b) in the event of dissolution or insolvency,
c) for failure to comply with this procedure or other legal obligations;
d) upon expiry of the validity of the documents provided for in Article 5(2)(b);
e) in the event of non-compliance with the measures ordered by the ADR following an inspection.

(2) Deregistration from the Register shall be communicated to the provider by the ADR.

Article 12. - (1) Providers issuing certificates for advanced electronic signatures shall be obliged to keep the data relating to the traceability of the certificates for a minimum period of 10 years and to ensure that the chain of trust is maintained.

(2) In the event of cessation of activity, the ADR shall ensure, as appropriate, that:

a) the certificates are revoked;
b) the records are transferred to another provider, with its consent;
c) all certificates are revoked if subparagraph (b) is not possible, at the expense of the provider.

ANNEX 2.1 to the procedure

Template application

for registration in the Register of non-qualified trust service providers

Dear Mr/Ms President,

The undersigned *[name of trust service provider]*, established at *[full address]*, registered with the Trade Register Office under No *[registration number/unique registration code]*, tax code [*CUI/CIF*], telephone [……], email [……], legally represented by *[name and surname]*, identified by [*identification document series, number, personal identification number*], pursuant to the provisions of Government Decision No 89/2020 and Law No 214/2024, hereby request registration in the Register of non-qualified trust service providers for the following trust service:

[*exact name of service*]

Short description of the service:

.....

.....

The system operates (or will operate) from the premises at *[full address, if different from the registered office]*.

Date: .....

Name and surname of applicant: .....

Signature (handwritten or qualified electronic signature): .....

Annex: The documentation provided for in Article 5(2) of the procedure, duly signed and numbered.

ANNEX 3

PROCEDURE

for the registration and deregistration of non-qualified trust service providers in the field of defence, public order and national security in the Register of non-qualified trust service providers

CHAPTER I Purpose, subject matter, scope and legal framework of the procedure

Article 1. (1) This procedure establishes the rules for the registration of legal persons in the field of defence, public order and national security that intend to provide non-qualified trust services, in the Register of non-qualified trust service providers, in accordance with Article 21 of Law No 214/2024.

(2) The provisions of the procedure shall also apply to closed systems, defined in Article 6 of Law No 214/2024, if entities in the field of defence, public order and national security choose to use them.

Article 2. The applicable legal framework is as follows:

e) 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, as subsequently amended and supplemented, hereinafter referred to as Regulation (EU) No 910/2014;
f) Law No 214/2024 on the use of electronic signatures, timestamps and the provision of trust services based on them, hereinafter referred to as Law No 214/2024;
g) Government Decision No 189/2025 on the organisation and functioning of the Ministry of the Economy, Digitalisation, Entrepreneurship and Tourism;
h) Government Decision No 89/2020 on the organisation and functioning of the Authority for the Digitalisation of Romania, as subsequently amended and supplemented.

CHAPTER II Powers of the Authority for the Digitalisation of Romania

Article 3. Pursuant to Article 21 of Law No 214/2024, the Authority for the Digitalisation of Romania (ADR):

f) maintains the Register of non-qualified trust service providers;
g) analyses registration applications and the associated documentation;
h) orders the registration of providers in the Register of non-qualified trust service providers;

i) checks providers' compliance with the applicable legal requirements;
j) asks for remedial measures to be implemented where non-conformities are identified.

CHAPTER III Registration of providers

Article 4. (1) Legal persons in the field of defence, public order and national security wishing to provide non-qualified trust services submit an application to the Romanian Digitalisation Authority (ADR) at least 30 days before the start of the activity, using the template provided in Annex 3.1, accompanied by the documentation provided for in paragraph (2), in order to be registered in the Register of non-qualified trust service providers.

(2) The application shall be accompanied by the following documents:

a) A self-declaration from the legal representative of the institution in the field of defence, public order and national security confirming the existence of an audit report, no older than 90 days, issued by a specialised body within the institution in compliance with the auditing principles. The internal audit shall be carried out in accordance with the technical standards specific to provision of the trust services and related security services. The audit report must show compliance with at least the following:
   (i) in the case of service providers issuing certificates for advanced electronic signature, ETSI Standard EN 319 411-1 V1.4.1 (2023-10) ESI Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements, or subsequent versions, and the conditions specified in Article 26(1) of Regulation (EU) No 910/2014, as subsequently amended and supplemented;
   (ii) in the case of trust service providers issuing advanced signature tools other than digital certificates, ETSI Standard EN 319 401 V2.3.1 (2021-05) – Electronic Signatures and Infrastructures (ESI), General Policy Requirements for Trust Service Providers, or later versions, and the conditions specified in Article 26(1) of Regulation (EU) No 910/2014, as subsequently amended and supplemented;
   (iii) ETSI TS 119 461 V2.1.1 (2025-02) – ESI; Policy and security requirements for trust service components providing identity proofing of trust service subjects, or subsequent versions, for Baseline LoIP minimum level.
b) Self-declaration by the legal representative regarding the existence of a security plan for the information system used, endorsed by the competent national authority in the field of cybersecurity and cyber defence, in accordance with Law No 58/2023.
c) The terms and conditions that the trust service provider undertakes to comply with vis-à-vis the end user.

d) The list of standards according to which operations are carried out, audited, assessed or certified (in accordance with Article 19a(2) of Regulation (EU) No 910/2014, where applicable).
e) The provider's web address.
f) A self-declaration by the legal representative showing that the penetration tests have been carried out, the period during which they were carried out and the fact that the identified vulnerabilities have been remedied.
g) A self-declaration by the legal representative attesting to the involvement of staff with adequate knowledge, experience and qualification, as well as the training plan, in accordance with Article 12(2)(e) of Law No 214/2024.
h) Minimum one precise source of time, linked to universal time, in compliance with the business continuity and disaster recovery requirements.
i) The terms and conditions with which the end-user undertakes to comply (where applicable and distinct from point c)).

Article 3. (1) The ADR shall examine the documentation within 30 days of receipt. If the legal conditions are met, the provider is registered in the Register provided for in Article 21 of Law No 214/2024 and the Decision granting the status of a non-qualified trust service provider is issued.

(2) Trust service providers issuing advanced electronic signature certificates shall, during the certificate applicant identification process, use means of identification that are regulated and recognised at national level, in accordance with Article 26(1) of Regulation (EU) No 910/2014, as subsequently amended and supplemented, and Article 6 of Law No 214/2024, where applicable.

CHAPTER IV Reporting obligations and subsequent changes

Article 4. (1) Trust service providers shall inform the ADR at least 30 days before the start of the internal audit activity and shall, upon request, allow the supervisory body to participate as an observer.

(2) Should there be any changes to the documents provided for in Article 4(2), the provider shall be obliged to notify the ADR within 60 days of the date on which those changes came into force and to submit the updated documents (originals or certified copies).

CHAPTER V Deregistration from the Register

Article 5. (1) Non-qualified trust service providers in the field of defence, public order and national security will be deregistered from the Register provided for in Article 21 of Law No 214/2024 in the following situations:

a) at their request;
b) in the event of non-compliance with the provisions of this procedure;
c) upon expiry of the validity of the documents provided for in Article 2(2)(a), if they have not been renewed;
d) failure to comply with the deadlines for resolving the measures ordered following the inspections carried out by the supervisory body.

(2) The ADR shall inform the provider of the deregistration decision and the reasons for it.

Annex 3.1 to the procedure

Template application

for registration in the Register of non-qualified trust service providers

(Field of defence, public order and national security)

Dear Mr/Ms President,

The undersigned *[name of trust service provider]*, established at *[full address]*, registered with the Trade Register Office under No *[registration number/unique registration code]*, tax code [*CUI/CIF*], telephone [……], email [……], legally represented by *[name and surname]*, identified by [*identification document series*, *number*, *personal identification number*], pursuant to the provisions of Government Decision No 89/2020 and Law No 214/2024, hereby request registration in the Register of non-qualified trust service providers for the following trust service:

[*exact name of service*]

Short description of the service:

.....

.....

The system operates (or will operate) from the premises at *[full address, if different from the registered office]*.

Date: .....

Name and surname of the applicant: .....

Signature (handwritten or qualified electronic signature): .....

Annex: The documentation provided for in Article 2(2) of this procedure, signed and numbered.

ANNEX 4

PROCEDURE

supervision, inspection and sanctioning of trust service providers

CHAPTER I General provisions

Article 1. (1) This procedure regulates the unitary framework for the supervision, inspection and sanctioning of trust service providers, in accordance with Article 19(1) of Law No 214/2024 on the use of electronic signatures, timestamps and the provision of trust services based on them (hereinafter referred to as Law No 214/2024).

(2) The Authority for the Digitalisation of Romania (hereinafter referred to as the ADR) has primary competence for inspection, in its capacity as a supervisory and regulatory body specialised in the field of trust services, within the meaning of Regulation (EU) No 910/2014.

(3) The institutions in the field of defence, public order and national security shall internally designate a supervisory body with the role of establishing, maintaining and supervising the way in which the activity of the non-qualified trust service provider is organised.

(4) The internal supervisory bodies provided for in paragraph (2) shall establish and maintain the relationship with the supervisory body provided for in Article 19(1) of Law No 214/2024.

Article 2. (1) This procedure shall apply to all trust service providers – qualified and non-qualified – operating on Romanian territory or providing trust services to persons located on Romanian territory, to the extent that inspection powers for the ADR are provided for in Law No 214/2024 and Regulation (EU) No 910/2014.

(2) In carrying out its duties, the ADR cooperates with other competent authorities, including the National Supervisory Authority for Personal Data Processing, if infringements of the rules on the protection of personal data are identified.

CHAPTER II Subject matter and performance of the inspection

Article 3. The objectives of the inspection performed by the ADR are as follows:

a) to monitor the compliance of providers' activities with the requirements and obligations laid down in Law No 214/2024 and Regulation (EU) No 910/2014;
b) to monitor and analyse the way in which trust services are organised and performed;
c) it may, ex officio or at the request of any interested person, or in the context of the periodic inspections, check or arrange for checks to be made of the compliance of the activities of a trust service provider as well as of the consistency of the information contained in the submitted documentation and the manner in which the provider operates.

Article 4. In carrying out its supervisory and inspection duties, the ADR shall:

a) cooperate with the National Supervisory Authority for Personal Data Processing if the check reveals infringements of the rules on the protection of personal data;
b) perform any other duties established under Regulation (EU) No 910/2014, with and through Law No 214/2024;
c) order remedial measures and sanctions in accordance with the legislation in force.

CHAPTER III Rights and obligations of the inspection staff

Article 5 The ADR may, with prior notification or without notification when there are reasonable indications of non-compliance with legislation or following the reporting of security incidents:

a) Perform inspections or require a conformity assessment body to perform a conformity assessment of qualified trust service providers, at the expense of those trust service providers, in order to confirm that they and the qualified trust services they provide meet the requirements provided for in the legislation in force.
b) Perform inspections on non-qualified trust service providers. To the extent that such an inspection results in the need for a new audit report to confirm that the services provided continue to meet the requirements provided for in the legislation in force, the ADR may require the submission of such an audit report issued by an auditor listed on the DNSC List of Validly Certified Cybersecurity Auditors (LASC). This provision shall not apply to the operators in Annex 3.

Article 6. In the performance of their duties, staff responsible for supervision and inspection shall have the following rights:

a) To have physical and logical access, in accordance with the competences established by legislative acts, to all of the premises from which the trust service provider operates.
b) To ask the representative of the trust service provider to provide any documents or materials containing data relevant to the subject matter of the inspection and request that copies thereof be made available to him in electronic form in order to substantiate the findings and measures ordered. The documents will be made available in electronic copy within a reasonable time that will be specified in the inspection report.
c) To benefit from specific training/professional training programmes on a regular basis, in relation to the legislation in the area of competence.

Article 7 When exercising their professional duties, the staff in charge of supervision and inspection shall be obliged to:

a) obtain data on the sites used by the trust service provider by consulting the National Trade Register Office or other official databases;
b) present the representative of the trust service provider being inspected, at the start of the supervisory and inspection action, with the service order/delegation/decision and identification confirming their capacity and status;
c) ask to see the single inspection register in accordance with the provisions of Law No 252/2003 on the unique control register and ensure its completion;
d) inform the representative of the trust service provider that the documents, material and other documents obtained during the inspection remain confidential;
e) base its findings, conclusions and measures on the documents, information and data acquired from the representatives of the trust service provider and those resulting from direct analysis, as well as other verifiable data and information.

CHAPTER IV Findings, remedial measures and penalties

Section 1: Findings and remedial measures

Article 8. (1) At the end of each inspection, the ADR staff shall write up the Inspection Report, which shall include, but not be limited to:

a) the subject matter and period of the inspection;
b) the service provider’s identification data;
c) the documents and systems checked;
d) any irregularities found, with an exact indication of which articles of Law No 214/2024, Regulation (EU) No 910/2014 or other rules have been infringed;

e) recommendations, deadlines for remediation and responsibilities;
f) remedial measures and sanctions (if applicable).

(2) The inspection report shall be signed by the inspection staff and approved by the President of the ADR.

Article 9. - (1) Should the trust service provider fail to fulfil any of the requirements provided for under the legislation in force, the ADR will require it to remedy the situation within a set period of time, which may not be longer than 60 days.

(2) In the case of qualified trust service providers, failure to comply with the deadline for remedy may lead to initiation of the procedure to suspend or withdraw the qualified status, in accordance with Annex 1, and to the application of the penalties provided for by law.

(3) In the case of non-qualified trust service providers, failure to comply with the deadline for remedy will lead to the application of penalties in accordance with Chapter VIII of Law No 214/2024.

Section 2: Penalties and liability

Article 10. The administrative penalties applicable to providers shall be established in accordance with the provisions of Law No 214/2024, Regulation (EU) No 910/2014 and Government Order No 2/2001 on the legal regime of administrative offences.

Annex 5

Rules for the approval of validation mechanisms

CHAPTER I Purpose, subject matter, scope and legal framework

Article 1. These Rules regulate the stages and conditions of approval, by the Authority for the Digitalisation of Romania (ADR), of the validation mechanisms provided for in Article 5(2) of Law No 214/2024, regarding checking the validity of advanced and simple electronic signatures, as well as advanced electronic seals, when they are contested or not recognised.

Article 2. (1) The Rules apply to legal persons who develop, supply or use advanced or simple electronic signature validation mechanisms and who wish to obtain official approval from the ADR.

(2) This normative framework complements the provisions of Regulation (EU) No 910/2014 and Law No 214/2024 on the validation of electronic signatures.

Article 3. The legal framework for the procedure is:

a) 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, as subsequently amended and supplemented, hereinafter referred to as Regulation (EU) No 910/2014;
b) Law No 214/2024 on the use of electronic signatures, timestamps and the provision of trust services based on them, hereinafter referred to as Law No 214/2024;
c) Government Decision No 189/2025 on the organisation and functioning of the Ministry of the Economy, Digitalisation, Entrepreneurship and Tourism;
d) Government Decision No 89/2020 on the organisation and functioning of the Authority for the Digitalisation of Romania, as subsequently amended and supplemented.

CHAPTER II Powers of the Authority for the Digitalisation of Romania

Article 4. In the exercise of the powers provided for in Article 5(2) of Law No 214/2024, the ADR:

a) receives and analyses applications for the approval of validation mechanisms;
b) checks the documentation;

c) decides whether to approve, reject or request additions.

CHAPTER III Approval procedure

Article 5. (1) Providers applying for approval of a validation mechanism shall submit a written request to the ADR together with the technical documentation.

(2) The technical documentation shall include at least the following:

a) validation criteria/standards compliant with ETSI standards or other recognised standards for advanced electronic signatures; this list shall include at least the applicable validation requirements of standard ETSI TS 119 101 V1.1.1 (2016-03) – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation, or later versions;
b) a detailed description of the validation method;
c) the trust service validation guide, specifying the attributes checked;
d) the audit report written up by an IT auditor from the List of IT auditors managed by the ADR and published on the ADR website.

Article 6. (1) The ADR shall review the application and documentation within 30 days.

(2) If the documentation is incomplete, the ADR may request additional information; the time frame for review being suspended until the additions have been received.

(3) Once the review has been finalised, the ADR shall issue an approval document, which shall be published on the official website of the ADR, under the dedicated section.

CHAPTER V Final provisions

Article 7. The ADR shall publish the validation methods and their related guidelines on its website in a list specifically created for this purpose.