



Identomat

COMPLIANCE GUIDE

Government & Public Services Compliance in Romania

COUNTRY **Romania**

INDUSTRY **Government & Public Services**

LAST UPDATED **21 October 2026**

KEY REGULATORS **Authority for the Digitalisation of Romania · Ministry of Internal Affairs (Directorate General for Persons Records) · National Cyber Security Directorate**

Key takeaways

- Romania's state digital identity rests on two tools: the electronic identity card (CEI), issued since 20 March 2025 with a chip that carries login and advanced-signature certificates, and ROeID, a free app-based login run by the Authority for the Digitalisation of Romania.
 - The identity card itself can only be obtained in person, because photo, fingerprints and signature are captured at the counter. Once issued, the card or ROeID gives remote access to public e-services.
 - Each public body that offers an online service must decide which identity assurance level it needs (low, substantial or high under EU rules) and have its identification system audited against it. ROeID is recognised by the EU at level substantial.
 - Public authorities must accept documents signed with EU-compliant electronic signatures. Companies that identify people remotely by video in Romania need an endorsement from the Authority for the Digitalisation of Romania first.
 - Government bodies are not covered by the anti-money laundering law, but their identity documents drive everyone else's checks: the new card does not print the home address, so firms must read it from the chip.
-

Romania's public sector is open to digital service delivery and is moving quickly: more than 2.8 million electronic identity cards had been issued by 19 October 2026, and dozens of public bodies already accept ROeID login. There is no licence to "operate" in this sector; instead, the rules govern how identity documents are issued, how citizens prove who they are online, and which trust services the state recognises.

The principal authorities are the Authority for the Digitalisation of Romania (ADR), which runs ROeID and supervises trust service providers; the Ministry of Internal Affairs, whose Directorate General for Persons Records governs identity cards; and the National Cyber Security Directorate for the security of public systems.

The biggest obstacle for a supplier or relying party is fragmentation: the card, ROeID, qualified signatures and video identification each have their own rules, and the European Digital Identity Wallet is due by December 2026 on top of them.

CONTENTS

- 1 Who regulates this sector
- 2 Licensing and authorisation
- 3 Identity framework (AML rules do not apply)
- 4 Identity verification and onboarding
- 5 Digital channels: what's different
- 6 Data protection and biometrics
- 7 Sector-specific obligations
- 8 Risk indicators and red flags
- 9 Enforcement and penalties
- 10 Recent changes and what to watch
- 11 What this means for identity verification
 - Sources

1 Who regulates this sector

Authority	Remit	Level	Official site
Authority for the Digitalisation of Romania (ADR)	Supervisory body for trust service providers under Law no. 214/2024; runs ROeID; endorses remote video identification providers; notified ROeID to the EU	National	adr.gov.ro
Ministry of Economy, Digitalisation, Entrepreneurship and Tourism	Approves by order the procedures for trust service provider status, supervision and sanctions (Order no. 102/2026)	National	Order 102/2026 via adr.gov.ro
Ministry of Internal Affairs, Directorate General for Persons Records (DGEP)	Identity documents and population records under OUG no. 97/2005; issues the authentication and advanced-signature certificates on the CEI	National, with local community records services	depabd.mai.gov.ro
National Cyber Security Directorate (DNSC)	Cybersecurity of networks and information systems under OUG no. 155/2024 (NIS 2), including central public administration	National	dnsc.ro

National Supervisory Authority for Personal Data Processing (ANSPDCP)	Data protection, including a dedicated sanctions regime for public bodies	National	dataprotection.ro
European Commission and EU legislature	eIDAS Regulation, European Digital Identity Wallet and implementing acts	Supranational	eur-lex.europa.eu

2 Licensing and authorisation

Public bodies need no licence to deliver services online. Authorisation questions arise for the private firms that supply identity and signature services to them, or that connect to state identity systems.

Trust service providers

A provider must notify ADR 30 days before starting activity (art. 10(2) of [Law no. 214/2024](#)) and hold professional liability insurance (art. 12(6)). Qualified status is granted by ADR under [Order no. 102/2026](#), which requires a conformity assessment at least every 24 months, with the report sent to ADR within 3 working days.

In force from 3 Apr 2026

Remote video identification

Providers registered in Romania may identify people remotely by video only after obtaining an ADR endorsement (aviz). Entities authorised in another EU member state may serve Romanian citizens under art. 4 of the 2021 norms. ADR publishes the list of approved third-party identity verifiers ([ADR](#)).

ROeID integration

An authority joins ROeID by signing a collaboration protocol with ADR, integrating in a test environment and receiving a production connection notice; ADR estimates two weeks to one month ([ROeID](#)). Romanian electronic signature providers may also integrate ROeID for remote identification before signing.

Register entries

ADR's register of qualified and non-qualified providers follows ADR President's Decision no. 163/2026 (Official Gazette no. 253 of 31 March 2026); providers must report changes to their registered data within 30 calendar days.

Issuing certificates without verifying identity is a contravention fined at 50,000 to 100,000 lei (art. 28(2)(e) of Law no. 214/2024), and ADR can suspend a provider or delete it from the register (art. 29).

3

Identity framework (AML rules do not apply)

Public authorities are not reporting entities under [Law no. 129/2019](#) on preventing and combating money laundering: the list in art. 5(1) covers credit and financial institutions, gambling operators, professionals and traders, not the state. Some authorities have specific roles instead: the National Agency for Fiscal Administration reports cash-control suspicions to the financial intelligence unit (art. 6(4)), and supervisors must inform it of facts linked to money laundering (art. 26(2)).

Identity in the public sector is governed by a separate framework:

- **Identity documents.** [Government Emergency Ordinance \(OUG\) no. 97/2005](#) on records, domicile, residence and identity documents of Romanian citizens, approved by Law no. 290/2005 and republished in Official Gazette Part I no. 719 of 12 October 2011. Art. 12(3) lists the identity documents: the identity card, the simple identity card (CIS), the electronic identity card (CEI), the provisional identity card and the old identity booklet, while valid. Art. 13(1) makes the document proof of identity, Romanian citizenship and, where applicable, domicile or residence.
- **Card certificates.** Art. 17¹, as amended by [Government Ordinance no. 12/2023](#) (Official Gazette no. 84 of 31 January 2023), splits issuance: the Ministry of Internal Affairs issues the authentication and advanced electronic signature certificates; a qualified trust service provider issues qualified signature certificates.
- **Electronic signatures and trust services.** [Law no. 214/2024](#) on the use of electronic signatures, time stamps and trust services (Official Gazette Part I no. 647 of 8 July 2024, in force 8 October 2024) implements the eIDAS Regulation and repealed Law no. 455/2001, Law no. 451/2004 and OUG no. 38/2020 (art. 35). It has not been amended as of October 2026.
- **Electronic identification.** eIDAS, as amended by [Regulation \(EU\) 2024/1183](#), applies directly and sets the European Digital Identity Wallet framework.

The state framework also shapes private-sector checks: Law no. 129/2019 accepts eIDAS electronic identification means as a reliable, independent source for customer verification (art. 11(1)(a)).

The electronic identity card

The CEI chip stores the holder's visible data and personal numeric code (CNP), parents' first names and place of birth, certificates for authentication or electronic signature, the facial image and two fingerprints (with exceptions), and the domicile and residence addresses. The address is not printed on the card; it is held only on the chip and can be updated without a new card (carteadeidentitate.gov.ro). Reading the chip requires the machine-readable zone or the 6-digit card access number (CAN); login uses a 4-digit PIN and signing a 6-digit PIN, and five wrong attempts deactivate each function ([PIN codes](#)). Fingerprints and the facial image are protected by Extended Access Control and readable only by designated authorities. The simple identity card has no chip and supports neither digital login nor signature.

ROeID

ROeID is ADR's single sign-on for citizens' dealings with public administration. Enrolment is done in the app: a photo of the identity card, a selfie and a 20-second video of prompted head movements with the original card shown, reviewed within 24 to 72 working hours ([ROeID FAQ](#)). Romania notified ROeID under eIDAS at level of assurance substantial, with ADR as notifying authority ([OJ C/2024/7543](#)). ROeID also lets a CEI holder sign PDFs by tapping the card on an NFC phone.

Assurance levels and remote proofing

Under art. 8 of the [ADR norms of 11 November 2021 on remote identification by video](#) (Decision no. 564/2021, Official Gazette no. 1119 of 24 November 2021), a public body offering online services must analyse the information on its platform and set the assurance level of the electronic identification it accepts under Implementing Regulation (EU) 2015/1502; if it uses video identification to issue eID means, it must audit the system against that level. The norms cover public sector bodies alongside trust service, payment and credit institutions, and allow either a real-time session with a human operator or recorded captures checked afterwards (art. 2). Checks include the document's condition and optical security features, tilting the document before the camera and comparing the laser photo with the ghost image (art. 17), and matching the person to the photo and data (art. 18).

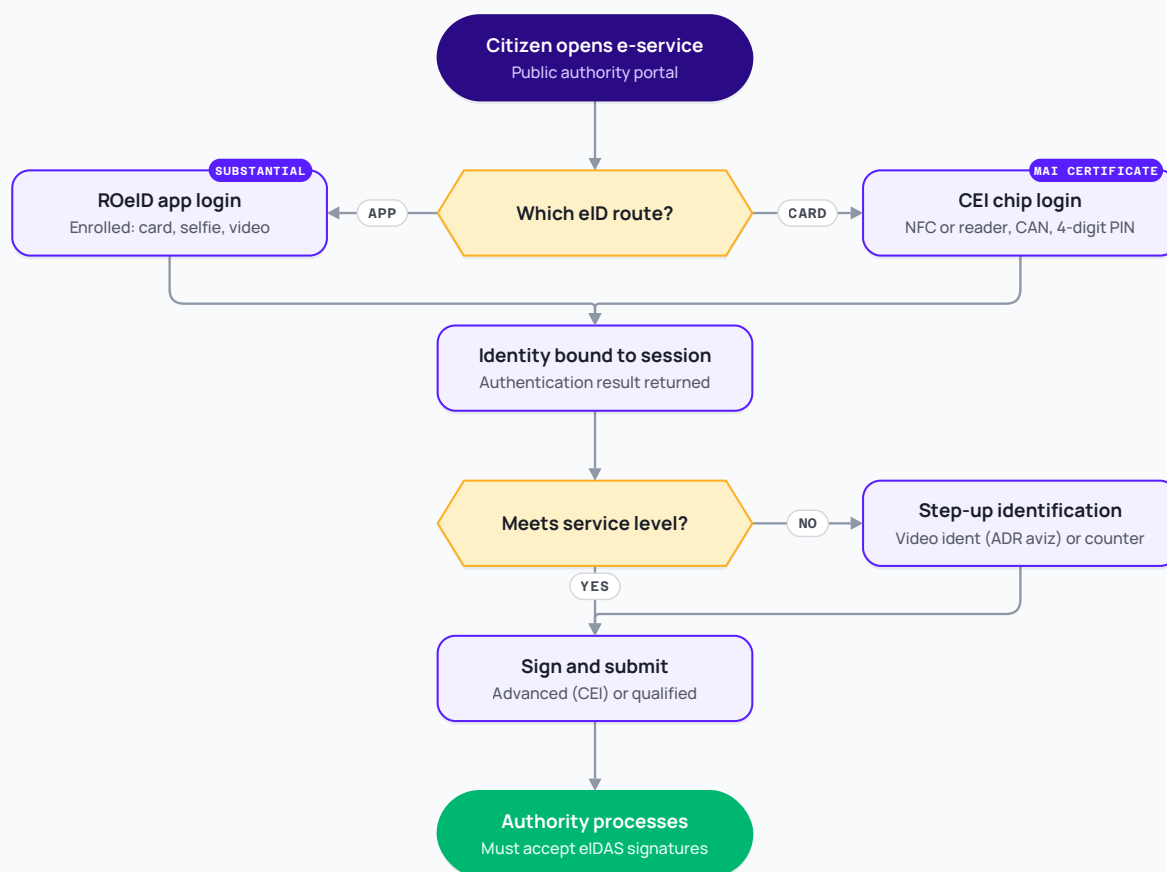


Figure 1. Remote access to a Romanian public e-service with electronic identity.

Qualified certificates

Before issuing a qualified or advanced-signature certificate, a provider verifies identity by one of the methods in art. 16(3) of Law no. 214/2024: physical presence with an original identity card, passport or residence permit; an existing qualified certificate; remote electronic identification at level substantial or high; other remote means with equivalent assurance under ADR norms; or a third-party verifier meeting those methods. Under Order no. 102/2026, non-qualified providers of advanced-signature certificates must use nationally recognised identification means and meet ETSI TS 119 461 at least at baseline level of identity proofing. Law no. 214/2024 also requires ADR to approve norms for other remote methods (art. 16(3)(d)); the 2021 video identification norms remain published as in force.

Bottom line: the identity document is always issued in person, but everything after issuance can be done remotely, and the remote route is governed by assurance levels the public body must set and audit.

Requirement	In person	Online / remote	Difference
Obtaining the identity card	Any community records service; photo, fingerprints and signature captured; no proxies	Not available; online appointment booking only	Differs
Proving identity to a public body	Show a valid identity document (art. 13 OUG 97/2005)	ROeID (substantial) or CEI authentication certificate with PIN	Differs
Assurance level	Physical presence	Set by the public body under Reg. 2015/1502 and audited (norms art. 8)	Differs
Proof of address	Read from the CEI chip with a reader or the RO CEI Reader app	Chip read by NFC, or a DGEP-signed electronic address certificate	Same
Signing a document	Handwritten signature	Advanced signature on the CEI, or qualified signature; authorities must accept (Law 214/2024 art. 25(1))	Differs
Issuing a qualified certificate	Physical presence before a trained representative (art. 16(3)(a))	eID at substantial or high, or equivalent means (art. 16(3) ©-(d))	Differs
Video identification providers	Not applicable	ADR endorsement required for providers registered in Romania	Differs
Data protection	GDPR and Law 190/2018	GDPR and Law 190/2018; consent to image capture kept with the video record	Same

Two state routes with different strengths

ROeID is an app account proofed by document photo, selfie and liveness video, recognised at level substantial. The CEI combines possession of the chip with a PIN and carries a Ministry of Internal Affairs advanced-signature certificate that the official card site describes as having the same value as a handwritten signature in Romania. A qualified signature, valid across the EU, can be added later by a qualified provider for a fee.

Address data moves to the chip

Because the CEI does not print the address, the financial intelligence unit (ONPCSB) reminds reporting entities that they must still obtain it, for example through the official RO CEI Reader app, which reads the chip and generates a PDF with the holder's PIN consent ([ONPCSB](#)).

Changes on the way

Each member state must provide at least one European Digital Identity Wallet within 24 months of the wallet implementing acts entering into force (art. 5a(1) of eIDAS as amended); [Implementing Regulation \(EU\) 2024/2979](#) entered into force on 24 December 2024, so the deadline falls in December 2026. Adopted, due Dec 2026 Where a public body requires electronic identification, it must then also accept the wallet (art. 5f(1)).

6 Data protection and biometrics

The GDPR applies directly, supplemented by [Law no. 190/2018](#) (Official Gazette Part I no. 651 of 26 July 2018). Three national rules bite on identity processing:

- **Biometrics.** Processing genetic, biometric or health data for automated decision-making or profiling needs the data subject's explicit consent or an express legal basis with safeguards (art. 3).
- **Personal numeric code.** Processing the CNP on the basis of legitimate interest requires safeguards, including technical and organisational measures, a data protection officer, storage limits and staff training (art. 4).
- **Public bodies.** ANSPDCP first issues a warning with a remediation plan (art. 13) and fines only if the plan is not carried out (art. 14).

For the CEI, fingerprints held in production databases are deleted automatically once the holder collects the card, or three months after the scheduled collection date ([carteadeidentitate.gov.ro](#)). In video identification, the person's consent to photographs and image capture is stored with the identification record under the 2021 ADR norms. Trust

service providers must keep issued certificates for at least 10 years after expiry (art. 16(2) of Law no. 214/2024) and comply with GDPR principles (art. 11(6)).

7 Sector-specific obligations

Accepting and issuing electronic documents

Public authorities must accept electronic documents signed in accordance with eIDAS and Law no. 214/2024 (art. 25(1)); if a portal cannot receive a document, e-mail may be used (art. 25(3)-(4)). Their own electronic acts must carry a qualified signature or an advanced signature based on a Romanian public-authority certificate (art. 24(1)). Heads of public authorities who breach art. 25(1) face fines of 5,000 to 50,000 lei (art. 32(2)).

Trust services feeding public systems

Trust service providers must integrate with the national interoperability platform to validate Romanian identity documents (art. 12(8)), keep records for at least 10 years, and keep a public online register of certificates (art. 14). Suspension or revocation must happen within 24 hours, with reasons given (art. 17).

Cybersecurity of public systems

[OUG no. 155/2024](#) (Official Gazette no. 1332 of 31 December 2024), approved by [Law no. 124/2025](#) (Official Gazette no. 638 of 7 July 2025), transposes the [NIS 2 Directive](#). Central public administration entities are essential entities regardless of size (art. 5(1)(a)), with listed exceptions such as defence, public order and national security institutions (annex 1, point 10). DNSC Orders nos. 1/2025, 2/2025 and 3/2025 set registration, risk methodology and supervision rules ([DNSC](#)). Under the Directive, qualified trust service providers are essential entities regardless of size.

IDENTITY ABUSE INDICATORS IN PUBLIC-SECTOR CHANNELS

- **Document fails optical checks:** damage, detectable falsification or missing visual security features (ADR norms art. 17).
- **Photo mismatch:** laser-printed photo differs from the ghost image, or the face does not match the person on video (arts. 17 and 18).
- **Card reported lost or stolen:** authentication certificates should be suspended or revoked; check status before relying on them.
- **Request for a PIN:** only the holder should know the 4-digit and 6-digit PINs; anyone asking for them is a warning sign.
- **Look-alike websites:** the official card site warns of clones; legitimate pages sit on the gov.ro domain.
- **Address taken from an old document:** the CEI address exists only on the chip, so printed proof may be outdated.
- **Real identity data in test systems:** names, CNPs and ID numbers exposed from a test server led to a 2026 fine.
- **Signing without consent:** using another person's electronic signature without their knowledge is a separate contravention (Law 214/2024 art. 31).

Regime	Who	Penalty basis
Law no. 214/2024, art. 28(1)	Trust service providers (e.g. failure to notify ADR)	15,000 to 75,000 lei per contravention
Law no. 214/2024, art. 28(2)	Providers, serious breaches including no identity check	50,000 to 100,000 lei; suspension or deletion (art. 29)
Law no. 214/2024, art. 31	Anyone using another's signature or seal without consent	75,000 to 100,000 lei

Law no. 214/2024, art. 32(2)	Heads of public authorities refusing eIDAS-signed documents	5,000 to 50,000 lei
OUG no. 155/2024, art. 60	Essential entities	10,000 lei up to 10 million euro or 2% of net turnover, whichever is higher, for the main breaches
Law no. 190/2018, arts. 13-14	Public bodies	Warning and remediation plan, then fines of 10,000 lei up to 200,000 lei depending on the breach
OUG no. 97/2005, art. 43(b)	Citizens (e.g. late identity card application)	500 to 1,000 lei, as amended by Law no. 14/2025

For important (rather than essential) entities under NIS 2, the top tier is 5,000 lei up to 7 million euro or 1.4% of net turnover. In a recent data protection case, ANSPDCP fined a private platform 31,451 lei after an attack on a test server that held real names, CNPs and identity document numbers, and ordered it to use only fictitious data in testing ([ANSPDCP, 16 October 2026](#)).

10 Recent changes and what to watch

- **19 August 2027** Adopted, applies 19 Aug 2027 [Implementing Regulation \(EU\) 2025/1566](#) makes ETSI TS 119 461 V2.1.1 the reference standard for verifying identity before issuing qualified certificates; remote proofing suppliers to qualified providers should test against it now.
- **December 2026** Adopted, due Dec 2026 Member states must provide a European Digital Identity Wallet; public bodies requiring eID must then accept it, and regulated private services follow within 36 months of the implementing acts (art. 5f(2)).
- **3 April 2026** In force Order no. 102/2026 replaced Order 449/2017 on trust service provider status; existing providers have 270 days, or until accreditation expires, to update their documentation.
- **31 March 2026** In force ADR Decision no. 163/2026 set the structure of the trust service provider register and a 30-day duty to report changes.
- **27 November 2025** In force DNSC Order no. 3/2025 set supervision and risk-based control rules for NIS 2 entities, including public administration.

- **7 July 2025** **In force** Law no. 124/2025 approved OUG no. 155/2024, confirming the NIS 2 framework for central public administration.
- **20 March 2025** **In force** Issuance of the electronic identity card began; the old 1997-model card stays valid until expiry but cannot be used as an EU travel document from 3 August 2031.

11

What this means for identity verification

- **Support several Romanian documents.** Valid identity documents include the CEI, the chipless simple card, older cards and the provisional card; only the CEI carries certificates and a chip.
- **Read the chip, not just the image.** Address and authentication data sit on the CEI chip behind the CAN or MRZ; NFC reading is the way to obtain them remotely.
- **Map each service to an assurance level.** Public bodies must set and audit the level; substantial (ROeID) or high determines which proofing methods are acceptable.
- **Video identification needs ADR endorsement.** A Romanian-registered provider cannot start without it, and must apply the document and face checks in arts. 17 and 18 of the 2021 norms.
- **Plan for the wallet.** Wallet acceptance becomes a public-sector duty from December 2026, and the ETSI TS 119 461 reference standard applies to qualified certificate proofing from August 2027.
- **Keep evidence and minimise data.** Store consent with video records, keep trust service records for 10 years, and never use real CNPs in test environments.

How Identomat helps

Identomat runs identity verification, screening and monitoring for regulated businesses on one platform, with workflows you configure for each market. For the requirements in this guide, that means:

- ID document capture and verification, including NFC chip reading of the Romanian electronic identity card and e-passports.
- Biometric liveness and face match for remote onboarding flows that must meet a defined assurance level.
- Video KYC sessions with recorded consent and an audit trail for each identification.
- No-code workflow builder to route citizens between eID login, step-up checks and e-signatures, with cloud, on-premises or hybrid deployment.

[Request a meeting](#)

DISCLAIMER

This article is intended for informational purposes only and does not constitute legal advice. It is a compilation of information from various sources and reflects the information available as of the last updated date indicated above. Laws, regulations, and regulatory guidance may change, so readers should consult qualified legal professionals for advice specific to their circumstances.

Sources

- **Legea nr. 214/2024 privind utilizarea semnăturii electronice, a mărcii temporale și prestarea serviciilor de încredere bazate pe acestea** [Law no. 214/2024 on electronic signatures, time stamps and trust services], Official Gazette Part I no. 647 of 8 July 2024, legislatie.just.ro; text linked from adr.gov.ro
- **Ordinul nr. 102/2026** [Order no. 102 of 29 January 2026 on trust service provider status, supervision and validation], Official Gazette no. 81 of 2 February 2026, and **Decizia ADR nr. 163/2026** [ADR Decision no. 163 of 20 March 2026 on the trust service provider register], Official Gazette no. 253 of 31 March 2026, both linked from adr.gov.ro
- **Norme din 11 noiembrie 2021 privind identificarea persoanei la distanță utilizând mijloace video** [ADR norms on remote identification by video, approved by Decision no. 564/2021], Official Gazette no. 1119 of 24 November 2021, legislatie.just.ro; ADR page adr.gov.ro

- **Ordonanța de urgență nr. 97/2005** [OUG no. 97/2005 on records, domicile, residence and identity documents of Romanian citizens], republished in Official Gazette no. 719 of 12 October 2011, consolidated text of 27 March 2025, legislatie.just.ro
- **Ordonanța nr. 12/2023** [Government Ordinance no. 12/2023 on population records and the electronic identity card], Official Gazette no. 84 of 31 January 2023, legislatie.just.ro
- **Directorate General for Persons Records, legal basis**, depabd.mai.gov.ro
- **Cartea electronică de identitate** [official electronic identity card site, Ministry of Internal Affairs]: [Despre](#), [Coduri PIN](#), [Utile](#)
- **ROeID** (Authority for the Digitalisation of Romania): [FAQ](#), [public administrations](#)
- **Electronic identification schemes notified pursuant to Article 9(1) of Regulation (EU) No 910/2014**, OJ C/2024/7543, eur-lex.europa.eu
- **Regulation (EU) 2024/1183** establishing the European Digital Identity Framework, arts. 5a and 5f, eur-lex.europa.eu
- **Commission Implementing Regulation (EU) 2024/2979** on the integrity and core functionalities of European Digital Identity Wallets, art. 15, eur-lex.europa.eu
- **Commission Implementing Regulation (EU) 2025/1566** on reference standards for verifying identity for qualified certificates, art. 2 and annex, eur-lex.europa.eu
- **Ordonanța de urgență nr. 155/2024** [OUG no. 155/2024 on the cybersecurity of networks and information systems], Official Gazette no. 1332 of 31 December 2024, arts. 5 and 60, annex 1, legislatie.just.ro; **Legea nr. 124/2025**, Official Gazette no. 638 of 7 July 2025, legislatie.just.ro; DNSC legislation page, dnsc.ro
- **Directive (EU) 2022/2555** (NIS 2), arts. 2 and 3, eur-lex.europa.eu
- **Legea nr. 190/2018** [Law no. 190/2018 on measures implementing the GDPR], Official Gazette no. 651 of 26 July 2018, arts. 3, 4, 13 and 14, legislatie.just.ro
- **ANSPDCP press release of 16 October 2026** (sanction for GDPR infringement), dataprotection.ro
- **Legea nr. 129/2019** [Law no. 129/2019 on preventing and combating money laundering], original text, arts. 5, 6, 11 and 26, asfromania.ro
- **ONPCSB, Obligations of the reporting entities** (notice on electronic identity cards), onpcsb.ro