



Identomat

COMPLIANCE GUIDE

Fintech & Digital Payments Compliance in Romania

COUNTRY **Romania**

INDUSTRY **Fintech & Digital Payments**

LAST UPDATED **21 October 2026**

KEY REGULATORS **National Bank of Romania · National Office for the Prevention and Combating of Money Laundering · Authority for the Digitalisation of Romania**

Key takeaways

- To provide payment services or issue electronic money (e-money) from Romania, you need an authorisation from the National Bank of Romania before you start; a firm already authorised in another EU or European Economic Area (EEA) country can instead passport in through a notification.
- Payment and e-money firms must identify every customer, verify identity, screen for politically exposed persons, monitor accounts and report suspicious transactions to Romania's financial intelligence unit before carrying them out.
- Fully remote onboarding is allowed: identity can be verified with EU-recognised electronic identification, qualified trust services, or video identification run under rules set by the Authority for the Digitalisation of Romania. Remote onboarding without such safeguards counts as a higher-risk factor.
- New Romanian electronic identity cards do not print the holder's address, so an app or website must obtain the address another way, for example by reading the card's chip with the holder's PIN.
- EU rules already on the calendar will change onboarding and payments: a single EU anti-money laundering rulebook applies from 10 July 2027, and Romanian payment and e-money institutions must handle instant euro transfers in 2027.

Romania is open to fintech and digital payment businesses, both locally authorised and passported from elsewhere in the EU. The licensing route is the standard EU one: Law 209/2019 for payment institutions and Law 210/2019 for e-money institutions, both administered by the National Bank of Romania (BNR), which is also the anti-money laundering supervisor for these firms.

The financial intelligence unit, the National Office for the Prevention and Combating of Money Laundering (ONPCSB), receives suspicious transaction and threshold reports. The consumer protection authority enforces the consumer-facing parts of the payment services law, and the Authority for the Digitalisation of Romania (ADR) sets the technical rules for remote video identification.

The biggest practical obstacle for a new entrant is building a remote onboarding journey that meets Romanian identification rules: an ADR-endorsed video identification process or an eIDAS electronic identification route, plus a way to capture the customer's address from the new chip-only identity cards.

CONTENTS

- 1 Who regulates this sector
- 2 Licensing and authorisation
- 3 AML, KYC and customer due diligence
- 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 for fintech	Level	Official site
National Bank of Romania (BNR)	Authorises and supervises payment institutions and e-money institutions; registers account information service providers; exclusive AML supervisor for these firms when they have a physical presence in Romania	National	bnr.ro
National Office for the Prevention and Combating of Money Laundering (ONPCSB)	Financial intelligence unit: suspicious transaction, cash and transfer reports; can suspend transactions	National	onpcsb.ro
National Authority for Consumer Protection (ANPC)	Enforces transparency and payment-rights provisions of Law 209/2019 where consumers are affected	National	anpc.ro
Authority for the Digitalisation of Romania (ADR)	Rules for remote identification by video; endorses video identification providers; supervises trust service providers	National	adr.gov.ro

National Supervisory Authority for Personal Data Processing (ANSPDCP)	GDPR supervision, including biometric and national identification number processing	National	dataprotection.ro
National Trade Register Office (ONRC)	Keeps the central register of beneficial owners	National	onrc.ro
European Banking Authority (EBA)	EU guidelines on payments, outsourcing and remote customer onboarding	Supranational	eba.europa.eu

2 Licensing and authorisation

Law no. 209/2019 on payment services (Legea nr. 209/2019 privind serviciile de plată, Official Gazette Part I no. 913 of 13 November 2019) prohibits anyone who is not a payment service provider from providing payment services on a professional basis (art. 8). A payment institution needs BNR authorisation before it starts (art. 9(1)), and BNR may authorise only a Romanian company with its real seat in Romania that provides at least part of its services there (art. 9(2)). BNR decides within three months of receiving a complete application (art. 26(1)).

Activity	Authorisation	Minimum initial capital
Money remittance only	Payment institution (Law 209/2019, art. 7(1)(f))	EUR 20,000 equivalent in lei (art. 18(1)(a))
Payment initiation only	Payment institution (art. 7(1)(g))	EUR 50,000 (art. 18(1)(b))
Accounts, cash, transfers, cards, acquiring	Payment institution (art. 7(1)(a) to (e))	EUR 125,000 (art. 18(1)(c))
Account information only	Registration with BNR as a specialised account information service provider (Title II, Chapter II)	Not applicable

Issuing e-money
(wallets, prepaid)

E-money institution (Law 210/2019, art. 7)

EUR 350,000 (art. 17)

Law no. 210/2019 on the issuance of electronic money (Official Gazette Part I no. 914 of 13 November 2019) applies the same model: a Romanian company with its real seat in Romania, authorised by BNR before issuing (art. 7). E-money issuers may not pay interest or any benefit linked to how long the holder keeps the e-money (art. 94). Both laws were last amended by Law no. 16/2025 (Official Gazette no. 234 of 17 March 2025), which aligned the operational and security risk provisions of Law 209/2019 with the EU Digital Operational Resilience Act (art. 218).

Passporting and agents

A payment institution authorised in another member state may operate in Romania through branches, agents or directly once its home authority notifies BNR (Law 209/2019, art. 56). A Romanian payment institution that wants to use an agent applies to BNR first (art. 48). EEA payment and e-money institutions serving Romania through agents or distributors remain responsible for AML compliance in that activity and must impose the AML framework on those agents by contract and check it (Law no. 129/2019, art. 5(2) and (3)).

Operating without authorisation

Providing payment services without being entitled to do so is a criminal offence punishable by six months to three years' imprisonment or a fine (Law 209/2019, art. 235(1)).

3

AML, KYC and customer due diligence

Payment and e-money institutions are reporting entities as financial institutions under Law no. 129/2019 on preventing and combating money laundering and terrorist financing (Official Gazette Part I no. 589 of 18 July 2019, consolidated to 19 December 2025), art. 5(1)(b). BNR has exclusive, risk-based AML supervision of Romanian payment and e-money institutions and of branches of EEA institutions with a physical presence in Romania (art. 27(1)). BNR Regulation no. 2/2019 (Official Gazette Part I no. 736 of 9 September 2019) sets the detailed requirements for BNR-supervised firms.

When due diligence applies

Standard customer due diligence (CDD) applies when a business relationship starts, for occasional transactions of at least EUR 15,000 (single or linked), for occasional transfers of

funds of at least EUR 1,000, and whenever money laundering or terrorist financing is suspected (art. 13(1)). For individuals, BNR Regulation 2/2019, art. 8(1) adds data such as the personal numeric code, address, occupation, source of funds and politically exposed person status.

Simplified and enhanced measures

Simplified measures are allowed only for customers rated low risk (art. 16(1)); products whose risk is contained by financial limits are one listed low-risk factor (art. 16(2)(b)). Enhanced measures are mandatory in higher-risk situations, including relationships with politically exposed persons, which continue for at least 12 months after the person leaves office (art. 17(1)). Business relationships or transactions conducted at a distance without safeguards such as electronic identification, relevant trust services or an ADR-approved remote process are listed as a higher-risk factor (art. 17(14)).

Reporting

Suspicious transactions

Report to ONPCSB before executing any related transaction; the transaction waits 24 hours from registration of the report, and ONPCSB may suspend it for up to 48 hours (arts. 6 and 8).

Cash

Cash transactions of EUR 10,000 equivalent in lei or more, including linked operations (art. 7(1)).

External transfers

Credit and financial institutions report transfers into and out of accounts to or from abroad of EUR 10,000 or more (art. 7(3)).

Money remittance

Remittance transfers of EUR 2,000 or more (art. 7(5)). Threshold reports are due within three working days of the transaction (art. 7(7)).

Beneficial ownership and records

Firms verify the beneficial owners of corporate customers against the central register kept by ONRC under art. 19 of Law 129/2019, or similar registers abroad (BNR Regulation 2/2019, art. 12). CDD records, including data obtained through electronic identification or ADR-approved remote processes, are kept for five years after the relationship ends or the occasional transaction is carried out (Law 129/2019, art. 21(1)).

Law 129/2019, art. 11(1) (a) requires verification from reliable, independent sources, including eIDAS (Regulation (EU) No 910/2014) electronic identification and trust services, or any secure remote process recognised or approved by ADR. BNR Regulation 2/2019, art. 11 points to documents hardest to forge, such as an official photo identity document, or electronic identification; other data is checked against credible sources such as the persons records, immigration and ONRC databases.

Video identification

The norms on remote identification by video, approved by ADR President's Decision no. 564/2021 (Official Gazette Part I no. 1119 of 24 November 2021), set minimum technical and security requirements. Providers registered in Romania may perform video identification only after ADR endorsement, issued within 30 days of a complete file (art. 3). Key requirements:

- a prior risk analysis (art. 13);
- explicit consent to the process and to photographs of the person and document (art. 16);
- document checks that include tilting the document and checking at least three security features of different categories (art. 17), and at least two features listed in the EU PRADO register by the system (art. 19(e));
- a random element in automated sessions to defeat pre-recorded video (art. 18); a live, uninterrupted session with a human operator, or a recording verified within 24 hours (art. 19(a));
- a mandatory one-time password or time-limited link sent by email or SMS before the process can close (art. 21);
- the whole session recorded and kept in a form admissible in court (art. 22).

Providers established in another member state may also serve Romania; the contracting firm is then liable for wrong identification and must hold EUR 100,000 of liability insurance (art. 4).

Addresses on electronic identity cards

ONPCSB has warned that some new electronic identity cards do not show the holder's address, which is a mandatory field in reports, and that firms must find another way to obtain it, for example the Ministry of Internal Affairs' RO CEI Reader app, which reads the chip, including the address, after the holder enters a PIN.

Reliance on third parties

Firms may rely on CDD performed by credit and financial institutions, but not on currency exchange offices, payment institutions providing only money remittance or payment initiation, account information service providers or postal payment providers (BNR Regulation 2/2019, art. 19).

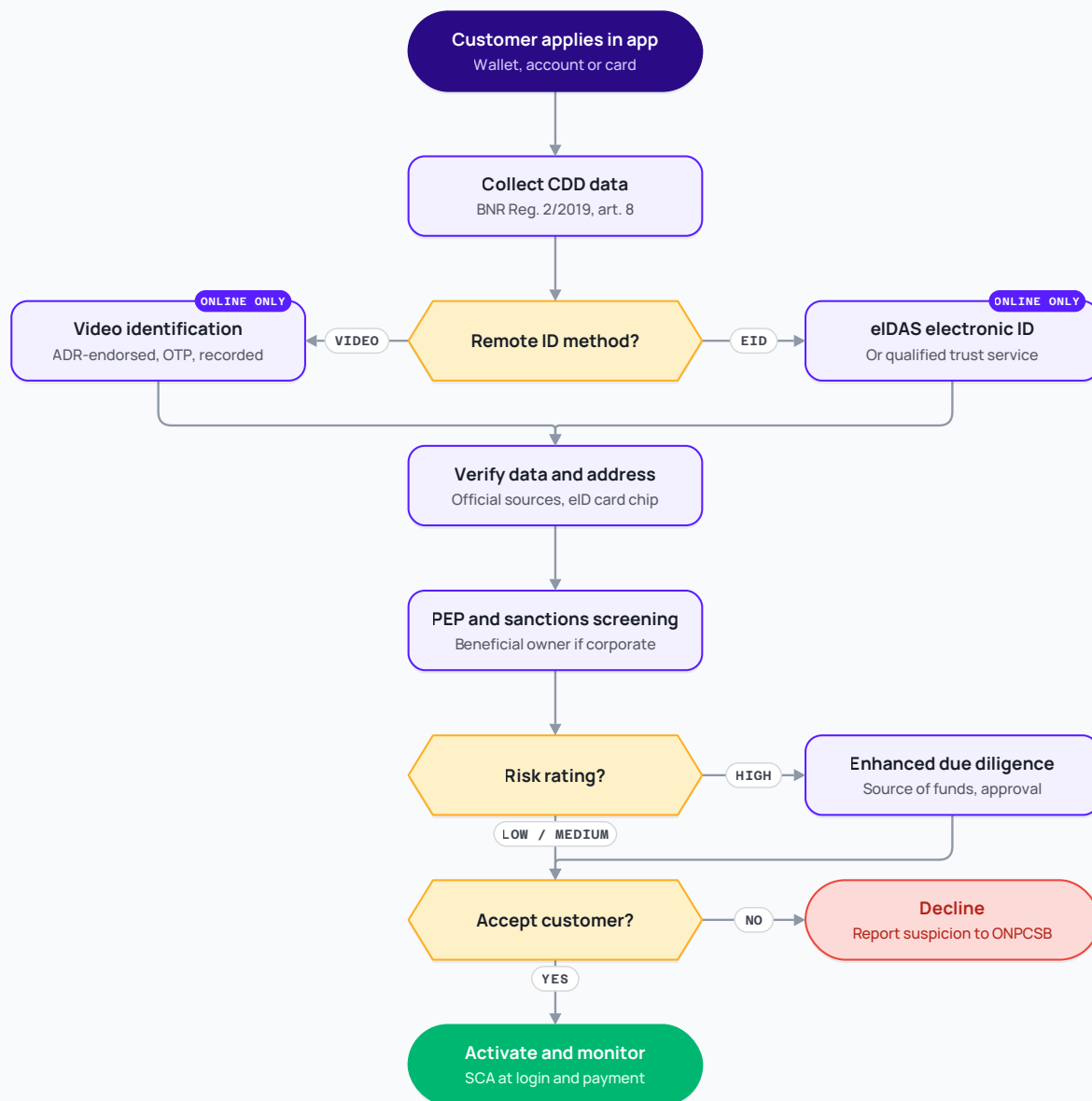


Figure 1. Remote onboarding of a retail customer by a Romanian payment or e-money institution.

Bottom line: the CDD obligations and thresholds are channel-neutral, but remote onboarding must use eIDAS electronic identification, a qualified trust service or an ADR-recognised process such as endorsed video identification; remote onboarding without those safeguards is treated as higher risk.

Requirement	In person / branch or agent	Online / remote	Difference
Who must be identified, and when	Relationship start; EUR 15,000 occasional; EUR 1,000 transfers	Same triggers	Same
Identity evidence	Official photo identity document	eIDAS eID, trust services or ADR-recognised remote process	Differs
Risk treatment	Risk-based	Remote without safeguards is a higher-risk factor	Differs
Video identification	Not applicable	ADR norms; ADR endorsement for Romanian providers	Differs
Address from new identity cards	Obtain by other means, such as chip reading	Obtain by other means, such as chip reading with PIN	Same
Record keeping	CDD records for 5 years	5 years, plus the full video session recording	Differs
Customer authentication	Not triggered by counter transactions	Strong customer authentication for online access, e-payments and risky remote actions	Differs
Reliance on another firm's CDD	Allowed, with exclusions	Same exclusions	Same

Remote identification routes

Law 129/2019, art. 11(1) (a) names three remote routes: eIDAS electronic identification, trust services and ADR-recognised processes, of which ADR's video norms carry the

detailed national procedure. The EBA Guidelines on remote customer onboarding (EBA/GL/2022/15), applicable since 2 October 2023, add EU expectations for the policies and testing behind any remote solution.

Strong customer authentication

Payment service providers must apply strong customer authentication when the payer accesses a payment account online, initiates an electronic payment, or takes any remote action that may carry a risk of fraud; remote electronic payments also need dynamic linking to the amount and payee (Law 209/2019, art. 220).

What is changing

From 10 July 2027, Regulation (EU) 2024/1624 **Adopted, applies 10 Jul 2027** will let firms verify identity with an identity document or with eIDAS electronic identification at assurance level substantial or high and relevant qualified trust services (art. 22(6)).

6 Data protection and biometrics

The GDPR applies directly, supplemented by Law no. 190/2018 on measures implementing it (Official Gazette no. 651 of 26 July 2018). Processing biometric data for automated decision-making or profiling is permitted only with the data subject's explicit consent or under express legal provisions with appropriate safeguards (art. 3(1)). Processing the personal numeric code (CNP), including by collecting copies of documents that contain it, must rest on a GDPR legal basis; where it rests on legitimate interests, the controller must apply safeguards such as data minimisation, security measures, a data protection officer and defined retention periods (art. 4).

For video identification, ADR's norms require express consent to the process and to image capture, stored with the identification record (art. 16).

7 Sector-specific obligations

Safeguarding customer funds

Payment institutions providing services under art. 7(1) (a) to (f) of Law 209/2019 must safeguard customer funds, either by segregating them and depositing them in a separate account or low-risk assets, or by insurance or a comparable guarantee; protected funds cannot be seized by other creditors, including in insolvency (art. 38). Emergency Ordinance

no. 5/2026 (Official Gazette no. 172 of 5 March 2026)

In force, pending parliamentary approval lets BNR open safeguarding accounts for payment institutions (art. 38(3)), as part of transposing the EU instant payments rules.

Instant euro payments and verification of payee

Under Regulation (EU) 2024/886, payment and e-money institutions in member states outside the euro area, such as Romania, must be able to receive instant euro credit transfers by 9 April 2027 and send them by 9 July 2027; verification of the payee applies to non-euro area providers by 9 July 2027. All providers offering instant euro transfers had to screen their users against EU targeted financial sanctions by 9 January 2025.

Consumer protection

ANPC enforces the transparency and rights provisions of Law 209/2019 where consumers are affected, with fines of 50,000 to 100,000 lei and 80,000 to 100,000 lei for repeat breaches within six months (arts. 230 and 231). Directive (EU) 2023/2225 on consumer credit, applicable from 20 November 2026, covers buy-now-pay-later offered through a third-party lender; only interest-free deferred payment granted by the supplier itself and repaid within 50 days is excluded (art. 2(2)(h)).

8 Risk indicators and red flags

Indicators from ONPCSB's money mule typology (December 2023) and its false identity documents case study:

PAYMENT AND E-MONEY TYPOLOGIES (ONPCSB)

- **New-account inflows:** receipts from many individuals shortly after the account is opened.
- **Pass-through:** credits matched by debits the same or next day; the account is used as a transit account.
- **Mirror transfers:** repeated receipts from one person, sent back the same day in the same amount.
- **Remittance corridors:** transfers labelled as gifts, medical treatment or visa fees to unrelated recipients, often in West Africa.
- **Profile mismatch:** salaried customer profile but activity unrelated to income or stated purpose.
- **Third-party card use:** signs that someone other than the holder uses the card linked to the account.
- **Forged identity documents:** accounts opened with false documents and funded from abroad, then emptied in cash.
- **Emailed instructions:** outgoing payments to unknown persons following instructions received by email.

9

Enforcement and penalties

For AML breaches by the firms it supervises, BNR applies administrative sanctions under Law 129/2019, art. 27(7) to (9), instead of the general fines in arts. 43 and 44:

- a written warning, or a public warning naming the person and the breach;
- a fine on the firm of up to 10% of total annual turnover (from the latest approved financial statements) or up to 23,000,000 lei;
- a fine of 10,000 to 23,000,000 lei on the responsible individual, and withdrawal of approval of directors or managers;
- orders to stop the conduct, temporary bans on responsible individuals holding functions in an institution, and withdrawal of the firm's authorisation.

For breaches of the payment institution rules, BNR may impose a written warning, a fine of 5,000 to 50,000 lei on the institution, fines of one to six average net monthly salaries on managers, withdrawal of managers' approval, or suspension or withdrawal of the authorisation (Law 209/2019, art. 77).

BNR publishes its AML sanctions. On 1 August 2025 (Order no. 82) it fined the Bucharest branch of iBanFirst SA 50,000 lei for breaches including the external transfer reporting rules and their three-day deadline (Law 129/2019, art. 7(3) and (7)) and ongoing monitoring (art. 11(1)(d)). On 27 February 2026 (Order no. 12) it issued a written warning to the digital bank Salt Bank S.A. for breaches of due diligence, risk assessment and internal control requirements.

10 Recent changes and what to watch

- **10 July 2027:** EU Anti-Money Laundering Regulation (EU) 2024/1624 applies
Adopted, applies 10 Jul 2027. A single EU rulebook replaces most national CDD detail.
- **9 April and 9 July 2027:** instant euro transfers and verification of payee for Romanian payment and e-money institutions under Regulation (EU) 2024/886
Adopted, applies 2027.
- **20 November 2026:** application date of Directive (EU) 2023/2225 on consumer credit
Adopted, applies 20 Nov 2026; affects credit-linked payment products.
- **5 March 2026:** Emergency Ordinance no. 5/2026 amends the safeguarding rules in Law 209/2019 **In force, pending parliamentary approval**.
- **17 March 2025:** Law no. 16/2025 amends Laws 209/2019 and 210/2019 **In force**.
- **EU Payment Services Regulation and third Payment Services Directive**
Proposed, EU procedure ongoing: would replace the current framework; no application date yet.

11 What this means for identity verification

- **Choose a recognised remote route.** For Romanian customers, use ADR-compliant video identification (through an endorsed or EU-established provider) or eIDAS electronic identification; document-and-selfie flows outside those routes leave remote onboarding classed as a higher-risk factor.
- **Build the video flow to ADR's checklist.** Randomised prompts in automated sessions, document tilting and security feature checks, a one-time password or expiring link, explicit consent and full session recording.
- **Plan for chip-only addresses.** New identity cards may not print the address, so read the chip (with the holder's PIN) or capture the address from another reliable source.

- **Collect BNR's data set**, including the personal numeric code, with Law 190/2018 safeguards.
- **Retain evidence for five years** after the relationship ends, including eID data and video recordings, in a form admissible in court.
- **Re-verify at risk points**: strong customer authentication at login and payment, and refreshed CDD when monitoring flags money mule patterns.

IDENTOMAT

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:

- Video KYC for remote onboarding, with document checks, liveness detection and full session recording for audit.
- ID document capture and verification, including NFC chip reading of electronic identity cards and passports.
- Biometric liveness and face match to confirm the customer is present and matches the document.
- AML screening against sanctions, PEP and adverse-media lists at onboarding and on an ongoing basis.
- No-code workflow builder to route customers to video identification or electronic ID and to enhanced due diligence by risk.

[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. 129/2019 pentru prevenirea și combaterea spălării banilor și finanțării terorismului** [Law 129/2019 on preventing and combating money laundering and terrorist financing], Official Gazette Part I no. 589 of 18 July 2019, consolidated form of 19 December 2025, arts. 2, 5, 6, 7, 8, 11, 13, 16, 17, 19, 21, 27, Legislative Portal, legislatie.just.ro
- **Regulamentul BNR nr. 2/2019 privind prevenirea și combaterea spălării banilor și finanțării terorismului** [BNR Regulation 2/2019 on AML/CFT], Official Gazette Part I no. 736 of 9 September 2019, consolidated, arts. 8, 11, 12, 19, legislatie.just.ro
- **Legea nr. 209/2019 privind serviciile de plată** [Law 209/2019 on payment services], Official Gazette Part I no. 913 of 13 November 2019, consolidated form of 5 March 2026, arts. 7, 8, 9, 18, 26, 38, 48, 56, 77, 218, 220, 230, 231, 235, 236, legislatie.just.ro
- **Legea nr. 210/2019 privind activitatea de emitere de monedă electronică** [Law 210/2019 on the issuance of electronic money], Official Gazette Part I no. 914 of 13 November 2019, as amended by Law 16/2025, arts. 7, 17, 94, legislatie.just.ro
- **Ordonanța de urgență nr. 5/2026** [Emergency Ordinance 5/2026 amending acts on credit institutions, capital adequacy and payment services], Official Gazette Part I no. 172 of 5 March 2026, legislatie.just.ro
- **BNR, Instituții de plată** [Payment institutions: legislation list], bnr.ro; **Instituții emitente de monedă electronică** [E-money institutions], bnr.ro
- **BNR, Sancțiuni aplicate și măsuri dispuse de BNR** [AML sanctions and measures published under art. 46 of Law 129/2019], Orders no. 82/2025 and no. 12/2026, bnr.ro
- **Norma din 2021 privind identificarea persoanei la distanță utilizând mijloace video** [ADR norms on remote video identification], approved by ADR President's Decision no. 564/2021, Official Gazette Part I no. 1119 of 24 November 2021, arts. 3, 4, 13, 16 to 22, linked from adr.gov.ro
- **ONPCSB, Obligațiile entităților raportoare** [Reporting entities' obligations: notice on new electronic identity cards and RO CEI Reader], onpcsb.ro
- **ONPCSB, Tipologie Money Mule**, December 2023, section III, onpcsb.ro; **Tipologii acte de identitate false, studiu de caz 1** [False identity documents typology], onpcsb.ro
- **Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679** [Law 190/2018 implementing the GDPR], arts. 3 and 4, dataprotection.ro
- **Regulation (EU) 2024/1624** on the prevention of the use of the financial system for money laundering or terrorist financing, arts. 22(6) and 90, eur-lex.europa.eu
- **Regulation (EU) 2024/886** as regards instant credit transfers in euro, art. 1 (new arts. 5a, 5c and 5d of Regulation (EU) No 260/2012), eur-lex.europa.eu
- **Directive (EU) 2023/2225** on credit agreements for consumers, arts. 2(2) (h) and 48, eur-lex.europa.eu
- **Procedure 2023/0210/COD**, proposal for a Regulation on payment services in the internal market, eur-lex.europa.eu

- EBA Guidelines on the use of remote customer onboarding solutions (EBA/GL/2022/15), applicable from 2 October 2023, eba.europa.eu