



Identomat

COMPLIANCE GUIDE

Banking & Digital Banking Compliance in Romania

COUNTRY **Romania**

INDUSTRY **Banking & Digital Banking**

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

- Only a licensed credit institution may take deposits from the public in Romania. A bank needs a National Bank of Romania licence and at least the lei equivalent of EUR 5 million in initial capital, or it can enter from another EU country on its home licence.
 - Fully remote account opening is allowed. A bank can verify a new customer by a video session, by an EU-recognised electronic identity, or by a qualified electronic signature, as long as the identity is checked before the account is opened.
 - Video identification carries Romania-specific steps: the bank must notify the Authority for the Digitalisation of Romania 30 days before using it, send a one-time code during the session, check security features of the identity card or passport, and record the whole session.
 - Remote onboarding without such safeguards counts as a higher-risk situation, so plan for extra checks when a customer cannot use a recognised remote method.
 - From 10 July 2027 the EU Anti-Money Laundering Regulation replaces most of the national customer due diligence rules with one EU rulebook; banks should design today's onboarding with that switch in mind.
-

Romania is open to digital and branchless banks, but the market is tightly licensed. The National Bank of Romania (BNR) authorises credit institutions, supervises them prudentially and, under the anti-money laundering law, is their exclusive anti-money laundering (AML) supervisor. Suspicious transaction and threshold reports go to the National Office for the Prevention and Combating of Money Laundering (ONPCSB), Romania's financial intelligence unit.

The biggest practical hurdle for a new digital entrant is not permission to onboard remotely, which the law grants, but the detail: the BNR expects remote onboarding to follow the European Banking Authority guidelines, video identification has its own national technical norms, and the newest identity cards no longer print the holder's address, which banks must still collect.

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

Regulator	Remit	Level	Official site
National Bank of Romania (BNR)	Licensing and prudential supervision of credit institutions; exclusive AML supervisor of banks, payment and e-money institutions; sanctions for AML breaches	National	bnr.ro
National Office for the Prevention and Combating of Money Laundering (ONPCSB)	Financial intelligence unit; receives suspicious, cash and external-transfer reports; publishes typologies	National	onpcsb.ro
Financial Supervisory Authority (ASF)	AML supervision of investment firms, asset managers, insurers and pension administrators	National	asfromania.ro
Authority for the Digitalisation of Romania (ADR)	Issues the norms on remote video identification, receives banks' notifications and keeps the list of third-party verifiers	National	Norms on legislatie.just.ro
National Trade Register Office (ONRC)	Central register of beneficial owners of companies	National	onrc.ro

National Supervisory Authority for Personal Data Processing	Data protection, including biometric and national identification number processing	National	dataprotection.ro
European Banking Authority (EBA)	Guidelines on risk factors and remote onboarding that the BNR applies	Supranational	eba.europa.eu

Deposits are protected by the Bank Deposit Guarantee Fund set up under Law no. 311/2015.

2 Licensing and authorisation

Government Emergency Ordinance no. 99/2006 on credit institutions and capital adequacy (OUG 99/2006) reserves deposit-taking to credit institutions: no other person may take deposits or other repayable funds from the public (art. 5(1)). Every credit institution operating in Romania needs an authorisation (art. 10(1)), and the BNR may not grant one unless initial capital is at least the minimum set by regulation, which cannot be lower than the lei equivalent of EUR 5 million (art. 11).

A credit institution authorised in another EU member state may serve Romanian customers through a branch or directly, without a Romanian licence, for the activities covered by its home authorisation (art. 45(1)). A passported bank still applies Romanian AML law to its activity here, and the BNR supervises the AML compliance of branches of foreign credit institutions (Law 129/2019, art. 27(1)(a)).

Deposits are covered up to the lei equivalent of EUR 100,000 per depositor (Law no. 311/2015, art. 61(3)). Brokerage and investment services sit with the ASF, which applies its own AML rule, ASF Regulation no. 13/2019; that regulation also treats video connection as a recognised way to verify a customer who is not physically present.

3 AML, KYC and customer due diligence

Credit institutions are reporting entities under Law no. 129/2019 on preventing and combating money laundering and terrorist financing (art. 5(1)(a)), consolidated to 19 December 2025. BNR Regulation no. 2/2019 sets out how banks apply it.

When due diligence applies

On opening a business relationship; occasional transactions of EUR 15,000 or more; transfers of funds of EUR 1,000 or more; on suspicion; and where earlier data is doubtful (Law 129/2019, art. 13(1)). Identity and beneficial owner must be verified before the relationship starts (art. 11(8)).

Data to collect

For individuals: name, date and place of birth, personal numeric code (CNP) or equivalent, address and its legal status, citizenship, occupation, contact details, purpose of the relationship, source of funds and politically exposed person status (Regulation 2/2019, art. 8(1)).

Enhanced due diligence

Mandatory for politically exposed persons (and for at least 12 months after they leave office), high-risk third countries, cross-border correspondent relationships and complex or unusual transactions; for politically exposed persons this means senior approval, source of wealth and funds, and enhanced monitoring (art. 17(1) and (9)).

Simplified due diligence

Only for customers rated low risk, never on suspicion, and identity and beneficial owner must still be identified and verified in every case (art. 16(4)-(5), as amended by Law no. 86/2025).

Beneficial ownership

A beneficial owner is any individual who ultimately owns or controls the customer; holding 25% plus one share is an indicator of ownership (art. 4(2)(a)). When onboarding a company, a bank must obtain proof of registration or an extract from the central beneficial owner register (art. 11(8¹)), kept by the ONRC for companies (art. 19(5)(a)), but may not rely on the register alone (art. 19(10)). Discrepancies between the register and the bank's own findings must be reported to the register (art. 19(7¹)).

Reporting and records

- **Suspicious transactions:** report to ONPCSB before executing the related transaction; the transaction is held for 24 hours, and ONPCSB may suspend it for up to 48 hours (art. 8(1), (3) and (4)).
- **Cash transactions** of EUR 10,000 or more, including linked operations (art. 7(1)).
- **External transfers** into or out of accounts of EUR 10,000 or more (art. 7(3)); both threshold reports within 3 working days (art. 7(7)).

- **Records:** customer due diligence records, including data from electronic identification, kept for 5 years after the relationship ends, extendable by up to 5 years on request, then deleted (art. 21).

Banks must appoint a compliance officer from senior management (art. 23(2)) and assess the risks of new products and technologies before launch (art. 25¹).

4 Identity verification and onboarding

Law 129/2019 lets a bank verify identity from reliable, independent documents, data or information, including EU electronic identification means and trust services under Regulation (EU) No 910/2014 (eIDAS), or any other secure remote or electronic identification process regulated, recognised, approved or accepted by the ADR (art. 11(1)(a)).

Regulation 2/2019 requires verification against documents that are hardest to forge, such as official photo identity documents, or through the electronic identification means the law allows (art. 11(1)). Other data can be checked against credible independent sources, including the databases of the persons records directorate, the immigration inspectorate and the ONRC (art. 11(2)).

Some new electronic identity cards do not show the holder's domicile. ONPCSB has reminded reporting entities that address collection remains mandatory and pointed to the Ministry of Internal Affairs' RO CEI Reader application, which reads the chip, including the address, with the holder's PIN.

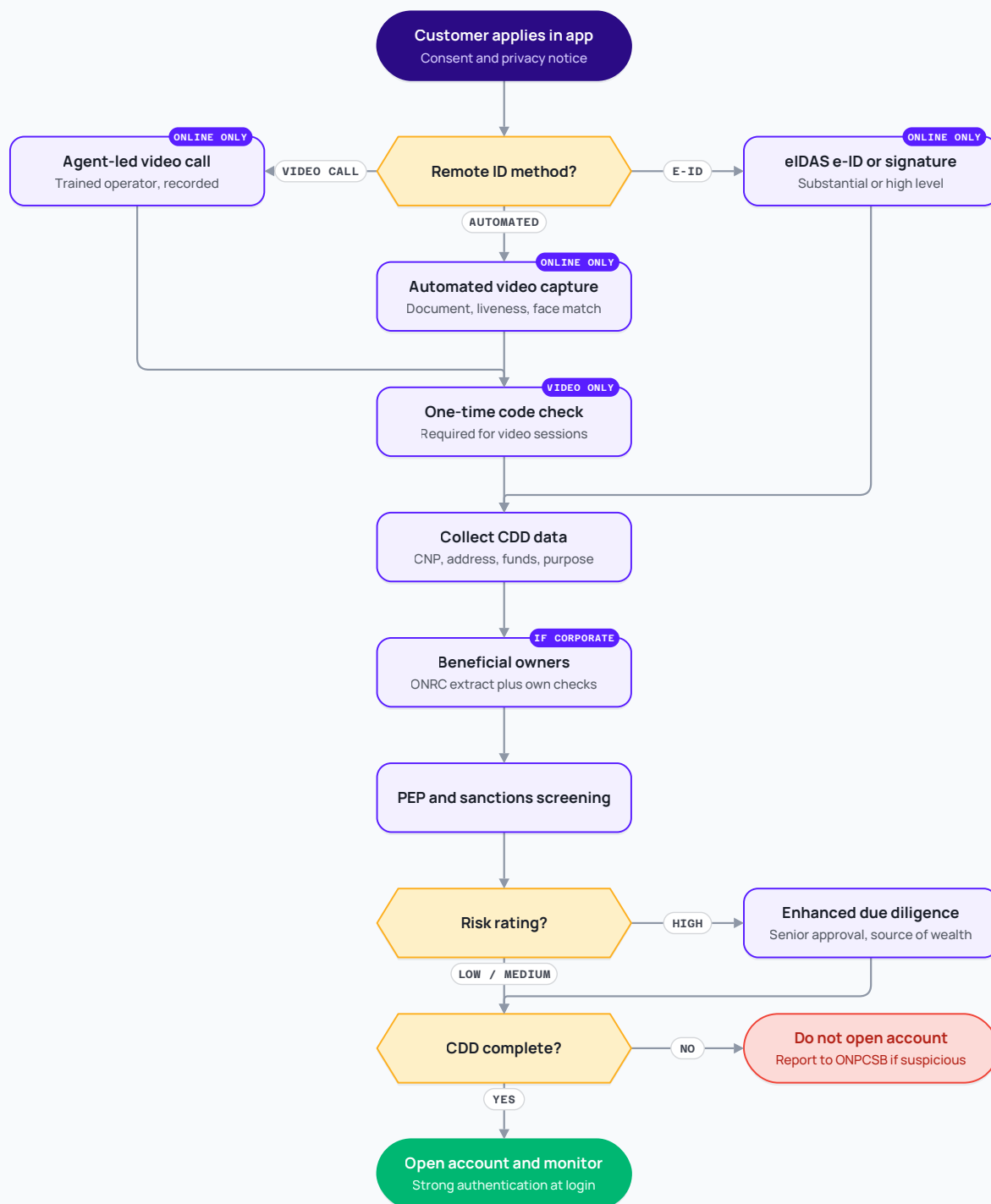


Figure 1. Remote account opening at a Romanian bank.

Video identification under the ADR norms

The Norms on remote identification by video means, approved by ADR President's Decision no. 564/2021, cover both live sessions with a human operator and recorded captures

without an operator that are verified afterwards, including automated, artificial-intelligence-based checks (art. 2©-(d) and 10(1)). For banks, the key rules are:

- Credit institutions must notify the ADR 30 days before first use, with a technical description, an IT audit report, third-party liability insurance of EUR 100,000 and policy declarations; a bank using a listed third-party verifier or qualified trust service provider files the contract instead (art. 7).
- Only a valid identity card or passport is accepted (art. 11 and annex 2).
- The system must check at least two security features from different categories listed in the EU's public register of authentic identity documents (PRADO); automated flows need a random element against pre-recorded attacks (art. 18(e) and 19(e)).
- A one-time password or time-limited link must be sent and validated before the session ends (art. 21), and the entire process is recorded and kept in a form admissible in court (art. 22).
- Poor image, light or sound, or doubts about the document, interrupt the session (art. 20).

Reliance on third parties

A bank may rely on due diligence performed by another credit or financial institution, but not by currency exchange offices, payment institutions offering only money remittance or payment initiation, account information service providers, or postal payment providers (Regulation 2/2019, art. 19). Responsibility stays with the relying bank (Law 129/2019, art. 18(5)), and outsourced due diligence must be contractually bound to the law (art. 18(8)).

5 Digital channels: what's different

Bottom line: the due diligence obligations are the same online and in a branch, but a remote relationship without a recognised safeguard (eIDAS identification, a trust service or an ADR-recognised process) is a statutory higher-risk factor, and video identification adds its own notification and technical rules.

Requirement	In branch	Online / remote	Difference
Remote onboarding permitted	Not applicable	Yes, via eIDAS means, trust services or ADR-recognised processes	Differs

Risk treatment	Risk-based	Higher-risk factor if no recognised safeguard is used	Differs
When identity is verified	Before the relationship starts	Before the relationship starts	Same
Accepted documents	Official photo ID, other documents and databases	Video: identity card or passport only	Differs
Process controls	Staff examine the original	Video: ADR notification, security-feature checks, one-time code, full recording	Differs
CDD data, including address	Full set under Regulation 2/2019	Same set; address from the identity card chip where not printed	Same
Record retention	5 years after the relationship ends	5 years, including electronic identification data	Same
Account access	Branch identification	Strong customer authentication for online access	Differs

The EBA remote onboarding guidelines are binding practice

BNR Instructions no. 2 of 3 April 2025 on the use of remote customer onboarding solutions require banks, payment and e-money institutions to take into account EBA Guidelines EBA/GL/2022/15. Those guidelines require liveness detection and strong face matching in unattended flows, trained staff and an interview guide in attended video calls, checks of document security features and of the machine-readable zone, consideration of chip (NFC) reading where technically possible, and redirection to face-to-face verification when evidence is ambiguous (paras. 33-42). eIDAS identification at substantial or high assurance, or qualified trust services, are treated as meeting the guidelines' data-quality and matching criteria (paras. 25 and 45).

Remote is not automatically high risk

Law 129/2019 lists remote relationships "without certain safeguards", such as eIDAS identification or an ADR-recognised process, among higher-risk factors (art. 17(14)(2)©). The BNR applies the EBA risk factor guidelines, which state that using electronic identification does not in itself increase risk (EBA/GL/2021/02, para. 4.31).

Account security

Once the account is open, Law no. 209/2019 on payment services requires strong customer authentication whenever a customer accesses the account online, initiates an electronic payment or takes any remote action carrying fraud risk (art. 220(1)).

Pending: **Applies 10 Jul 2027** the EU Anti-Money Laundering Regulation allows verification either by identity document or by eIDAS identification at substantial or high level plus qualified trust services (Regulation (EU) 2024/1624, art. 22(6)).

6 Data protection and biometrics

The General Data Protection Regulation (GDPR) applies directly, supplemented by Law no. 190/2018. Processing for AML purposes is a task in the public interest and may not be reused for commercial purposes (Law 129/2019, art. 22(1) and (4)); banks must give new customers a privacy notice, including a general notice of their AML obligations, before the relationship starts (art. 22(2)-(3)).

Biometric data used for automated decision-making or profiling, such as an automated face match, may be processed only with the customer's explicit consent or under an express legal provision with appropriate safeguards (Law 190/2018, art. 3(1)). The ADR norms also require express consent to the identification, its purpose and the capture of images of the person and the document, stored with the recording (art. 16). After the 5-year AML retention period, personal data must be deleted unless another law requires otherwise (Law 129/2019, art. 21(4)).

7 Sector-specific obligations

Correspondent banking

Banks may not maintain correspondent relationships with shell banks (Law 129/2019, art. 10(4)). Before opening a cross-border correspondent relationship with a respondent that executes payments for its own customers, the bank must assess the respondent's business, supervision and AML controls, obtain senior approval and document each party's responsibilities (art. 17(7)); some of these checks may be treated as met for respondents in other member states (art. 17(8)).

Anonymous products and existing customers

Banks may not offer anonymous accounts, passbooks or safe deposit boxes, or accept payments made with anonymous prepaid cards (art. 10(1), as amended by Law 86/2025). Where due diligence cannot be completed, the bank must not open the account or continue the relationship and must consider a suspicious transaction report (art. 11(9); Regulation 2/2019, art. 18).

Sanctions

EU restrictive measures apply directly. Under Government Emergency Ordinance no. 202/2008, everyone must take due diligence measures to ensure that transactions respect international sanctions, including asset freezes, and report implementing measures to the competent authorities (art. 18). The BNR supervises banks' sanctions compliance.

8

Risk indicators and red flags

RETAIL AND DIGITAL BANKING INDICATORS

- **Remote relationship without safeguards:** no eIDAS or ADR-recognised verification (Law 129/2019, art. 17(14)).
- **Avoiding face-to-face contact** or reluctance to provide due diligence information (EBA/GL/2021/02, para. 9.6).
- **Money mule activity:** accounts used to receive and pass on third-party funds, a typology ONPCSB has published.
- **False or altered identity documents** presented at onboarding, another ONPCSB typology.
- **Payments from unknown or unassociated third parties** (Law 129/2019, art. 17(14); EBA/GL/2021/02, para. 9.4).
- **Sudden activity after dormancy** or unexplained high-value banknote movements (EBA/GL/2021/02, para. 9.6).
- **Opaque ownership**, nominee shareholders or bearer shares (Law 129/2019, art. 17(14)).
- **Links to high-risk or sanctioned jurisdictions** (Law 129/2019, art. 17(14) (3)).

Enforcement and penalties

The BNR sanctions serious, repeated or systematic breaches of the core AML obligations, failures to follow its supervisory measures, and the start or continuation of relationships in breach of the law (Law 129/2019, art. 27(7)). Available sanctions are:

- a written or public warning;
- a fine on the institution of up to 10% of total annual turnover (based on the latest approved financial statements) or up to RON 23,000,000;
- a fine on responsible individuals of RON 10,000 to RON 23,000,000;
- withdrawal of approval of directors, temporary bans, or withdrawal of the licence (art. 27(8)-(9)).

The BNR weighs gravity, duration, culpability, financial strength and cooperation (art. 27(11)); the limitation period is 5 years (art. 27(10)).

The BNR publishes its decisions. On 27 February 2026 it issued Salt Bank S.A. a written warning for breaches including ongoing monitoring, unusual transaction review and risk assessment, together with 11 remedial measures covering alert handling, system parameters and controls on transfers lacking payer information. On 1 August 2025 it fined IBAN FIRST SA Bruxelles, Bucharest branch, RON 50,000, partly for failures in external transfer reporting ([BNR sanctions register](#)).

Recent changes and what to watch

- **Applies 10 Jul 2027** **EU Anti-Money Laundering Regulation (EU) 2024/1624**: replaces most national due diligence rules with a directly applicable EU rulebook; remote verification through eIDAS means is written into the text.
- **Transposition due** **Directive (EU) 2024/1640**: provisions on beneficial owner registers were due by 10 July 2026 and the rest by 10 July 2027; expect amendments to Law 129/2019 and to register access.
- **Wallet acceptance pending** **European Digital Identity Wallets**: banks that must use strong authentication will have to accept them, at the customer's request, within 36 months of the Commission's implementing acts of November 2024 (Regulation (EU) 2024/1183, art. 5f(2)).
- **In force** **26 May 2025, Law no. 86/2025**: bans acceptance of anonymous prepaid cards, requires identification and verification even under simplified due diligence, adds

pre-launch risk assessment of new products and technologies, and limits public beneficial owner register access to a legitimate interest.

- **In force** 3 April 2025, BNR Instructions no. 2/2025: banks must apply the EBA remote onboarding guidelines.
- **In force** 13 March 2025, OUG no. 10/2025: due diligence for transfers of funds from EUR 1,000 and BNR supervision of banks providing crypto-asset services.

11 What this means for identity verification

- **Documents:** for video flows, accept only valid Romanian identity cards and passports, check at least two PRADO security features, and read the machine-readable zone.
- **Address:** plan to read the domicile from the electronic identity card chip, or from another source, because it may not be printed on the card.
- **Liveness and matching:** unattended capture needs liveness detection, a random challenge and strong face matching; keep the full recording, time-stamped.
- **Extra factor:** build a one-time code or time-limited link into every video session.
- **Consent and vendors:** store explicit biometric consent with the session; a verifier on the ADR list simplifies notification, but the bank stays responsible.
- **Future-proofing:** support eIDAS substantial and high identification now; it is also an explicit route under the 2027 EU rulebook.

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:

- Remote account opening with ID document capture and verification, including NFC chip reading of electronic identity cards and passports.
- Video KYC with agent-led or automated sessions, biometric liveness and face match, and a full recorded audit trail.
- KYB and beneficial owner verification for corporate customers.
- AML screening against sanctions, PEP and adverse-media lists at onboarding and through ongoing monitoring.
- Phone and email verification for one-time codes, and a no-code workflow builder to route customers between remote methods.

[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 no. 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. 4, 5, 7, 8, 10, 11, 13, 14, 16-19, 21-25¹, 27, legislatie.just.ro
- **Regulamentul BNR nr. 2/2019 privind prevenirea și combaterea spălării banilor și finanțării terorismului** [BNR Regulation no. 2/2019], Official Gazette Part I no. 736 of 9 September 2019, as amended by Regulation no. 11/2022, arts. 8, 11, 18, 19, 21, legislatie.just.ro
- **BNR, Prevenirea spălării banilor și a finanțării terorismului** [AML legislation page, listing Instructions no. 2 of 3 April 2025 on remote customer onboarding solutions and Instructions of 14 August 2024 on risk factors], bnr.ro; text of the Instructions, [bnr.ro \(PDF\)](#)

- **BNR, Sancțiuni aplicate și măsuri dispuse de BNR** [Sanctions and measures imposed by the BNR], bnr.ro
- **Normele privind reglementarea, recunoașterea, aprobarea sau acceptarea procedurii de identificare a persoanei la distanță utilizând mijloace video** [Norms on remote identification by video means], approved by ADR President's Decision no. 564/2021, Official Gazette Part I no. 1119 of 24 November 2021, arts. 2, 7, 10, 11, 16-22 and annex 2, legislatie.just.ro
- **OUG nr. 99/2006 privind instituțiile de credit și adecvarea capitalului** [Government Emergency Ordinance no. 99/2006 on credit institutions and capital adequacy], Official Gazette Part I no. 1027 of 27 December 2006, arts. 5, 10, 11, 39, 45, legislatie.just.ro
- **Legea nr. 311/2015 privind schemele de garantare a depozitelor și Fondul de garantare a depozitelor bancare** [Law no. 311/2015 on deposit guarantee schemes], Official Gazette Part I no. 918 of 11 December 2015, art. 61(3), legislatie.just.ro
- **OUG nr. 202/2008 privind punerea în aplicare a sancțiunilor internaționale** [Government Emergency Ordinance no. 202/2008 on the implementation of international sanctions], art. 18, legislatie.just.ro
- **Legea nr. 209/2019 privind serviciile de plată** [Law no. 209/2019 on payment services], Official Gazette Part I no. 913 of 13 November 2019, art. 220, legislatie.just.ro
- **Law no. 190/2018 on measures implementing Regulation (EU) 2016/679**, art. 3, National Supervisory Authority for Personal Data Processing, dataprotection.ro
- **ONPCSB, Noile cărți de identitate** [The new identity cards], onpcsb.ro
- **ONPCSB, Tipologii** [Typologies], onpcsb.ro
- **ASF Regulation no. 13/2019 on measures to prevent and combat money laundering and terrorist financing**, consolidated 20 December 2023, asfromania.ro (PDF)
- **EBA/GL/2022/15, Guidelines on the use of remote customer onboarding solutions**, 22 November 2022, applicable from 2 October 2023, paras. 25, 33-45, eba.europa.eu (PDF)
- **EBA/GL/2021/02, Guidelines on ML/TF risk factors** (consolidated, as amended by EBA/GL/2023/03), paras. 4.29-4.34, 9.4-9.10, eba.europa.eu (PDF)
- **Regulation (EU) 2024/1624 on the prevention of the use of the financial system for money laundering or terrorist financing**, OJ L 2024/1624, 19 June 2024, arts. 22(6) and 90, eur-lex.europa.eu
- **Directive (EU) 2024/1640**, art. 78 (transposition), eur-lex.europa.eu
- **Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 (European Digital Identity Framework)**, art. 5f(2), eur-lex.europa.eu