Identomat

COMPLIANCE GUIDE

Banking & Digital Banking Compliance in Moldova

COUNTRY Moldova

INDUSTRY Banking & Digital Banking

LAST UPDATED 5 November 2026

KEY REGULATORS National Bank of Moldova · Office for Prevention and Fight against Money Laundering

Key takeaways

- Only a bank licensed by the National Bank of Moldova (NBM) may take deposits from the public. A foreign bank can take deposits in Moldova only through a branch the NBM has licensed, so a cross-border digital bank cannot simply collect deposits from abroad.
- Remote (fully online) account opening is allowed, but only for Moldovan citizens and for resident companies whose representatives, founders, directors and ultimate owners are all Moldovan citizens. Foreign nationals still have to be identified in person.
- Approved remote methods are a qualified electronic signature, a live video or live photo session with presence (liveness) checks and recording of the original identity document, or a service from a qualified trust service provider. The bank must notify the NBM 30 days before it starts using any remote onboarding solution.
- A law adopted in 2025 will extend remote onboarding to European Union (EU) citizens holding a qualified certificate, but it only takes effect once the supporting technical conditions are in place; no date had been set as of November 2026.
- From 17 March 2027 the new crypto-asset law lets banks issue e-money tokens and (meeting art. 17) asset-referenced tokens and, after notifying the CNPF 40 working days ahead, provide only custody and transfer of the tokens they issue themselves; they cannot extend to other crypto-asset services. However, the AML law's ban on virtual asset services had not been repealed as of November 2026. Today dealings with foreign virtual asset providers are capped at 50,000 lei a month per resident client.

Moldova's banking market is open to new entrants, but entry is through a full NBM bank licence or a licensed branch of a foreign bank; there is no lighter digital-bank licence. The NBM is the licensing, prudential and anti-money laundering (AML) supervisor for banks, and the Office for Prevention and Fight against Money Laundering (SPCSB) is the financial intelligence unit that receives reports.

The biggest obstacle for a digital-first entrant is the citizenship limit on remote identification: an app-only onboarding journey can serve Moldovan citizens, but every other customer must be identified with a physical presence until the EU extension takes effect.

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 Moldova (NBM)	Bank licensing, prudential supervision, resolution, AML supervision of banks, e-KYC rules	National	bnm.md
Office for Prevention and Fight against Money Laundering (SPCSB)	Financial intelligence unit; receives suspicious, cash and threshold reports; AML training and certification	National	spcsb.md
National Commission for Financial Markets (CNPF)	AML supervisor of investment firms, registries and fund managers; crypto-asset market authority with the NBM from 2027	National	cnpf.md
Bank Deposit Guarantee Fund (FGDSB)	Deposit guarantee scheme; every licensed deposit-taking bank is a member	National	fgdsb.md
State Tax Service	Receives notices on frozen assets and suspected circumvention of international restrictive measures	National	sfs.md
National Center for Personal Data Protection (CNPDCP)	Data protection supervisory authority	National	datepersonale.md

The Information and Security Service (SIS) supervises qualified trust service providers used for remote identification. Moldova is evaluated by MONEYVAL: its fifth-round report

was adopted in July 2019, with enhanced follow-up reports in May 2022, May 2024 and June 2025.

2 Licensing and authorisation

Under the Law No. 202 of 6 October 2017 on the activity of banks (last amended by Law No. 180/2026, effective 17 March 2027), every bank needs an NBM licence (art. 8), only banks may take deposits from the public (art. 6(1)), and only licensed banks and branches may use the word "bank" (art. 7).

Foreign banks

Deposit-taking only through an NBM-licensed branch; a representative office is notified but may not do banking business (art. 6(3) and (4)).

Initial capital

At least the NBM minimum, never below 100 million lei, fully paid in cash (art. 9).

Two-stage process

The NBM grants or refuses prior approval to establish the bank within 5 months of a complete application. The applicant then has 5 months to file the licensing documents, and the NBM decides within 2 months (art. 17).

Deposit guarantee

Deposits are covered up to 200,000 lei per depositor per bank from 1 January 2025 (Law No. 160 of 22 June 2023, art. 24). Membership of the scheme is mandatory from the date the licence takes effect.

There is no separate digital-bank licence: an app-only bank needs the same licence.

3 AML, KYC and customer due diligence

Banks are reporting entities under art. 4(1)(a) of the Law No. 308/2017 (last amended by Law No. 146/2026, in force 13 August 2026) and are supervised for AML by the NBM (art. 15(1)(a)). The NBM's detailed rules are in the Regulation on AML/CFT requirements in the activity of banks, approved by NBM Decision No. 200 of 9 August 2018 (last amended by NBM Decision No. 8 of 13 January 2025, in force 16 January 2025).

When customer due diligence applies

Standard CDD applies when a relationship starts; for occasional transactions over 20,000 lei in a single operation through payment service providers or over 200,000 lei in linked operations; on suspicion of money laundering or terrorist financing; and when earlier identification data is in doubt (Law 308, art. 5(1)). Cash currency exchange above 10,000 lei requires an identity document (Regulation 200, point 25). If CDD cannot be completed, the bank must refuse or end the relationship and report to the SPCSB (art. 5(3)). Anonymous accounts and relationships with shell banks are prohibited (art. 5(4)).

Data elements

For individuals: name, date and place of birth, citizenship, identity document data including the personal identification number (IDNP), address, occupation, source of income, beneficial owner and the purpose and expected volume of the relationship. Legal entities add registration documents, state identification number (IDNO), representatives and senior managers (Regulation 200, point 26).

Beneficial ownership and refresh cycle

A beneficial owner is a natural person holding more than 25% of capital or 25% plus one share, directly or indirectly, or exercising control by other means; if none is found, the senior administrator is recorded (art. 5^2). Banks must refresh customer and beneficial owner data at least annually for high-risk customers, every 2 years for medium risk and every 3 years for low risk (Regulation 200, point 39).

Reporting tiers and retention

Report to the SPCSB	Threshold	Deadline
Suspicious activity or transaction	Any amount	Immediately, within 24 hours
Cash activity or transactions	200,000 lei or more in a calendar month (single or linked)	By the 5th of the following month
Single non-cash transaction	200,000 lei or more	By the 10th of the following month
Money remittances (banks and payment firms)	Equivalent of 40,000 lei or more	Within 5 days

Records, including data from electronic identification, are kept for 5 years after the relationship ends, extendable by up to 5 more years on request (art. 9).

Targeted financial sanctions

Banks freeze assets of persons on the UN Security Council and EU terrorism lists, the UN proliferation list and the Information and Security Service's supplementary list, and inform the SPCSB within 24 hours (Law 308, art. 34(1), (4) and (11)). Under the Law No. 25 of 4 March 2016 on international restrictive measures, they block funds of subjects of international restrictions and inform the State Tax Service within 24 hours (art. 28(1)), and report suspected circumvention within the same period (art. 6(6)).

4 Identity verification and onboarding

In a branch, customers present original or certified identity documents (Regulation 200, point 38). Remote identification follows art. 5^1 of Law 308 and the NBM Regulation on requirements for identifying and verifying customers by electronic means (NBM Decision No. 281 of 7 November 2024, the e-KYC Regulation), which applies to banks, life insurers, non-bank credit organisations and payment and e-money firms.

Who may be onboarded remotely

Remote identification is limited to Moldovan citizens and resident legal persons whose representatives, founders, administrators and beneficial owners are all citizens (Law 308, art. 5^1(1); e-KYC Regulation, point 13). It may be used only for new customers or to update data of existing ones (points 12 and 30).

Accepted methods

Depending on risk, the bank uses one or more of: a qualified electronic signature; live video and audio with physical-presence checks, recording of the original identity document and capture of the face; a live photo with presence checks and the original document; or another electronic method offered by a qualified trust service provider accredited under Law No. 124/2022 (point 21).

Technical requirements

- Automated sessions need liveness or motion detection, document authenticity checks (security features, Machine Readable Zone), face matching, and must block pre-recorded uploads (point 23).

- Capture at 8 megapixels or Full HD at least (points 22 and 23), on solutions certified to standards such as ISO/IEC 30107 and NIST SP 800-63 (point 29).
- Device data is captured and the phone or email confirmed by one-time password before completion (points 24 to 26); sanctions, terrorist list, PEP and adverse-information checks are part of the session, and suspected coercion requires an in-person visit (point 28).

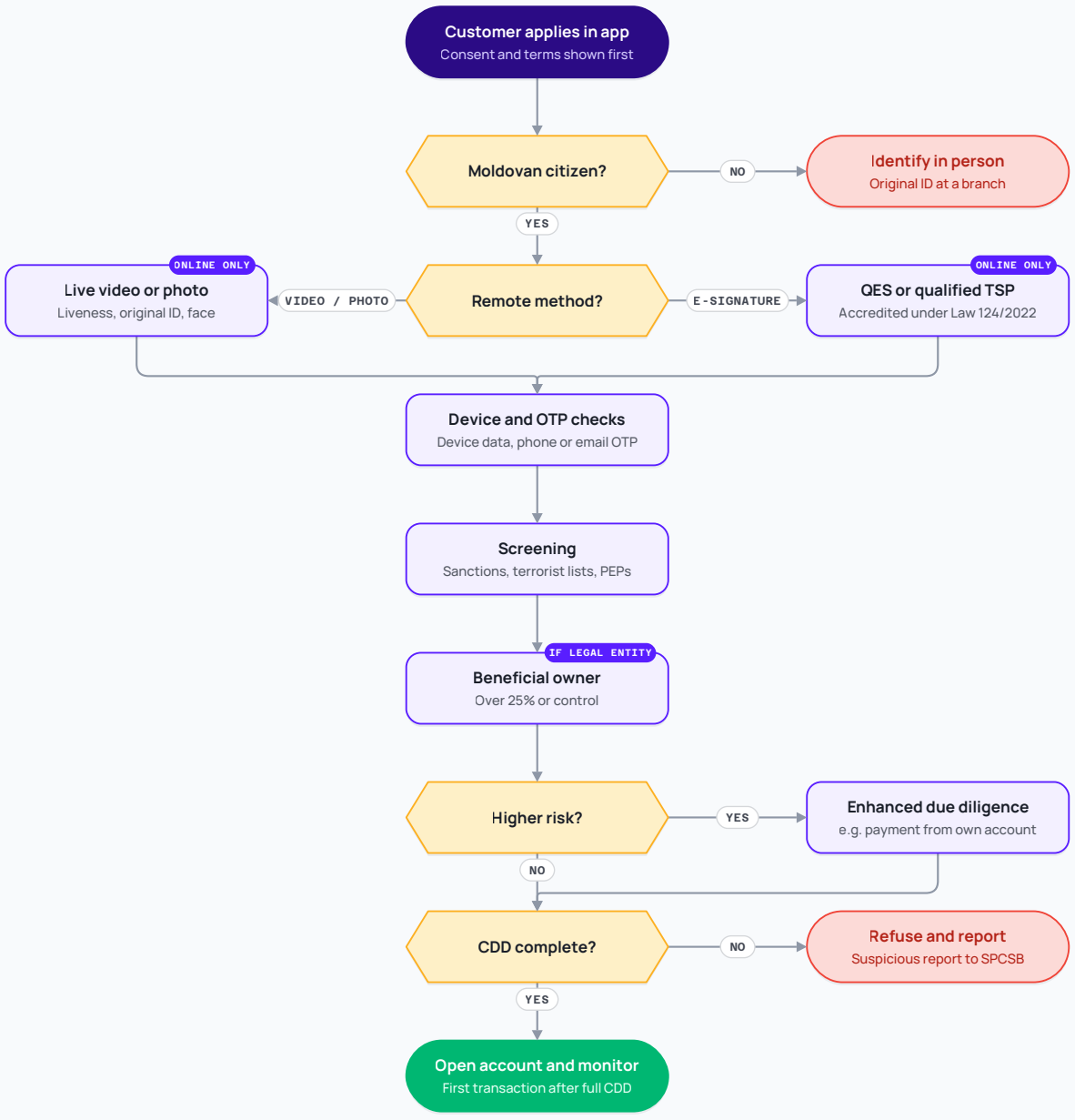


Figure 1. Remote account opening at a Moldovan bank under the NBM e-KYC Regulation.

A bank may rely on another supervised entity's CDD if the data is available immediately and the third party is not in a high-risk jurisdiction; final responsibility stays with the bank (Law 308, art. 10). Outsourcing remote identification follows the general outsourcing rules (e-

KYC Regulation, point 51): under the NBM Regulation on outsourcing of bank activities (Decision No. 46/2020, last amended by Decision No. 29 of 12 February 2025), the bank keeps final responsibility (point 6) and notifies the NBM within 10 working days of outsourcing a material activity, attaching the contract (point 38).

5 Digital channels: what's different

> **Bottom line:** remote account opening is legal and regulated in detail, but it is limited to Moldovan citizens and requires prior notice to the NBM, certified technology and fuller digital evidence than a branch visit.

Requirement	In person / branch	Online / remote	Difference
Who can be onboarded	Any customer, resident or not	Moldovan citizens and all-Moldovan resident companies only	Differs
Identity evidence	Original documents or certified copies	QES, live video or photo with presence checks, or qualified trust service	Differs
Risk treatment	Risk-based	Not-present customers are a high-risk factor unless identified electronically; extra EDD cases apply	Differs
Supervisor notice	None	Notify the NBM 30 days before launch	Differs
Location and network controls	Not applicable	Controls against IP masking, VPNs and proxies; unusual location monitored	Differs
Evidence kept	Documents and copies, 5 years	Also video, audio, photos, screenshots, device fingerprint and IP, 5 years	Differs
Account access	Not applicable	Strong customer authentication for online access and payments	Differs
Sanctions and PEP screening	Required	Required	Same

Reporting thresholds	Law 308, art. 11 tiers	Same tiers	`Same`

Risk treatment of remote customers

Law 308 lists customers who do not present themselves in person as a higher-risk factor, "with the exception of clients identified by electronic means" (art. 8(3), letter c), so a compliant e-KYC session does not by itself trigger enhanced due diligence. Enhanced measures still apply to applicants previously exited for failed CDD, residents of high-risk jurisdictions and trustees (point 38), using controls such as a first payment from the customer's own account elsewhere or extra biometric comparison (point 34).

Launching a remote solution

The bank tests the solution, including fraud and VPN detection (point 6), notifies the NBM 30 days before launch (point 49) and stops if the NBM finds significant risks (point 52). The first transaction runs only after full CDD (point 5(d)).

Account access after onboarding

As payment service providers under the Law No. 114 of 18 May 2012 on payment services and electronic money, banks apply strong customer authentication (two independent factors) to online access, electronic payments and risky remote actions (art. 52^4). Exemptions in the NBM Regulation on strong customer authentication (Decision No. 12/2024) include remote payments up to 600 lei within cumulative limits and balance views, which still need full authentication at least every 180 days (points 18, 19, 31).

Pending changes

Law No. 144 of 19 June 2025, art. XII, extends remote identification to EU citizens holding a qualified certificate issued by an EU trust service provider `Adopted, effective date not yet set`. It takes effect only once technical conditions for identification through qualified providers under Government Decision No. 977/2023 are in place (art. XVIII). Matching NBM changes to the e-KYC Regulation, covering high-assurance e-ID and the EVO government app, remain a draft `Draft, consultation closed 2 Mar 2026`.

6 Data protection and biometrics

The Law No. 195 of 25 July 2024 on personal data protection has applied since 23 August 2026 and replaced Law No. 133/2011, which older AML texts still cite. Biometric data used to

uniquely identify a person is a special category whose processing is prohibited unless an exception applies, such as explicit consent (art. 9).

The e-KYC Regulation requires consent to data processing before electronic identification starts (point 19) and a privacy notice, terms of use and short AML policy shown upfront (point 20). Video, audio, photos, screenshots, document copies, device fingerprint and IP address are kept for the life of the relationship and 5 years after it ends (point 46). Breaches of the core processing principles carry fines of up to 2,000,000 lei or 2% of total turnover, whichever is higher (art. 88(2)); under a phase-in, 10% of a fine set by the CNPDCP applies in the first year, 40% in the second and the full amount from the third (art. 90(4)).

7 Sector-specific obligations

Virtual asset restrictions

Providing virtual asset services in Moldova is currently prohibited (Law 308, art. $4(1^1)$). Banks may not hold accounts for or at foreign virtual asset providers, open non-resident accounts to deal with them, or run occasional transactions with them (art. $5(4^1)$ to (4^3)). Transactions of resident clients with providers authorised abroad may not exceed 50,000 lei a month in total (art. $5(4^4)$, inserted by Law No. 66/2023); for banks, Regulation 200, point 57^1 applies this cap through dedicated accounts and specialised monitoring and bars occasional transactions. From 17 March 2027 banks may issue e-money tokens and (meeting art. 17) asset-referenced tokens and, after notifying the CNPF 40 working days ahead, provide only custody and transfer of the tokens they issue themselves (Law No. 180/2026, art. 54(1)); they cannot extend to other crypto-asset services (art. 53(8)). Law 180 does not amend Law 308; it requires the Government to propose aligning legislation within six months of publication (art. 104(4)).

Correspondent relationships

Cross-border correspondent banking is higher risk; banks assess the respondent's management, activities and AML controls (Regulation 200, points 55 and 59).

AML staff certification

Law No. 146 of 23 July 2026 added art. 13^1 to Law 308: the senior manager responsible for AML, the compliance officer and compliance staff must hold a valid training certificate, renewed at least every 3 years. Firms get up to 3 months to remedy a gap. The SPCSB issues the national certificate after a one-week course and a Saturday exam; holders of

recognised AML certifications or at least 3 years' AML experience may apply for direct admission to the exam (SPCSB training page).

Securities-side onboarding

The CNPF supervises investment firms; its AML Regulation (Decision No. 63/1 of 19 December 2023) applies in-person identification standards to remote customers, with verified electronic signatures and an independent contact channel (point 59).

8 Risk indicators and red flags

HIGHER-RISK FACTORS AND FRAUD SIGNALS FOR MOLDOVAN BANKS

- **Remote relationships without safeguards**: distance relationships with no electronic signature or equivalent protection (Law 308, art. 8(3)(j)).
- **Unusual geography**: significant distance between bank and customer, or abnormal or high-risk device location during onboarding (art. 8(3)(a); e-KYC Regulation, point 9).
- **Compromised identity data**: identity elements on lists of stolen or compromised data, or known remote-onboarding fraud scenarios (point 9).
- **Session tampering**: signs that session confidentiality, integrity or authenticity was compromised, or use of VPNs and proxies to hide location (points 9 and 16).
- **Money mules**: accounts or cards opened for someone else in exchange for payment, with stolen funds withdrawn quickly or converted to crypto (SPCSB notice, 10 June 2026).
- **Third-party payments**: funds received from unknown or unrelated third parties (art. 8(3)(k)).
- **Virtual asset flows**: transactions with virtual asset providers authorised in other states (art. 8(3)(q)).
- **Opaque structures**: nominee shareholders, shares in custody or unusually complex ownership (art. 8(3)(e) and (g)).

9 Enforcement and penalties

Under Law 308, art. 35, AML breaches can bring public statements, cease orders, licence suspension or withdrawal, management bans and fines of up to double the benefit or the lei equivalent of EUR 1,000,000; for banks the ceiling is the lei equivalent of EUR 5,000,000 or 10% of prior-year turnover, under the procedure in Law No. 75/2020.

Under Law 202/2017, art. 141, the NBM may fine a bank up to 5% of own funds or 10% of net annual turnover, fine managers 1 to 100 average salaries, and withdraw the licence; the limitation period is 3 years (art. 142(3)).

The NBM's sanctions table shows that in 2026 it fined Banca de Finanțe și Comerț 7,696,934.85 lei (Decision No. 67 of 19 March 2026, including credit transfer and ICT breaches) and B.C. Comerțbank 958,369.16 lei (Decision No. 216 of 9 September 2026).

10 Recent changes and what to watch

- **17 March 2027**: Law No. 180/2026 lets banks issue e-money tokens and (meeting art. 17) asset-referenced tokens and, after notifying the CNPF 40 working days ahead, provide only custody and transfer of the tokens they issue themselves (art. 54(1)); they cannot extend to other crypto-asset services (art. 53(8)) `Adopted, effective 17 Mar 2027`.
- **26 October 2026**: SPCSB drafts of a new AML law and sanctions procedure law, to apply from 10 July 2027 and repeal Law 308 `Draft, consultation closed 2 Nov 2026`. They would accept e-ID at substantial or high assurance without a citizenship limit (draft art. 22(9)) and raise maximum fines for credit and financial institutions to at least EUR 10 million or 10% of turnover.
- **21 October 2026**: CNPF began drafting rules on how financial entities notify their intention to provide crypto-asset services `Drafting started, input due 5 Nov 2026`.
- **23 August 2026**: Law No. 195/2024 on personal data protection applies `In force`.
- **13 August 2026**: Law No. 146/2026 requires certified AML training every 3 years for compliance roles `In force`.
- **16 February 2026**: NBM draft amending the e-KYC Regulation (high-assurance e-ID, eIDAS and EUDI Wallet, EU citizens) `Draft, consultation closed 2 Mar 2026`.
- **20 June 2025**: Law No. 144/2025 extends remote identification to EU citizens with a qualified certificate `Adopted, effective date not yet set`.

11 What this means for identity verification

- **Citizenship gate**: route non-citizens to a branch; read citizenship and IDNP from the document.
- **Checks**: certified liveness, document and face matching.
- **Evidence**: keep recordings, device data and IP until 5 years after exit.
- **Re-verification**: every 1, 2 or 3 years by risk, and when data is in doubt.

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:

- Remote onboarding with ID document capture and verification, face match and biometric liveness, matching the automated method in the NBM e-KYC Regulation.
- Video KYC with a trained operator for the live video method, with recorded sessions kept as audit evidence.
- AML screening against sanctions, terrorist and PEP lists at onboarding and ongoing monitoring afterwards.
- KYB and beneficial owner verification for resident legal entities, plus phone and email verification for the one-time password step.
- No-code workflow builder to route non-citizens to an in-branch path and apply enhanced due diligence to higher-risk applicants.

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. 308 din 22.12.2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului** [Law No. 308/2017 on preventing and combating money laundering and terrorist financing], arts. 4, 5 (incl. 5(4^4)), 5^1, 5^2, 8, 9, 10, 11, 13^1, 15, 34, 35, State Register of Legal Acts, legis.md
- **Legea nr. 146 din 23.07.2026 pentru modificarea unor acte normative (consolidarea cadrului instituțional și certificarea în domeniul prevenirii și combaterii spălării banilor)** [Law No. 146/2026], art. I(3), art. III, MO 375-378/13.08.2026, legis.md
- **Legea nr. 144 din 19.06.2025 pentru modificarea unor acte normative (susținerea economiei digitale și a serviciilor electronice)** [Law No. 144/2025], arts. XII and XVIII, MO 328/20.06.2025, legis.md
- **Legea nr. 202 din 06.10.2017 privind activitatea băncilor** [Law No. 202/2017 on the activity of banks], arts. 4, 6 to 9, 14, 17, 141, 142, legis.md
- **Legea nr. 160 din 22.06.2023 cu privire la garantarea depozitelor în bănci** [Law No. 160/2023 on deposit guarantees], art. 24, legis.md; Bank Deposit Guarantee Fund, fgdsb.md
- **Hotărârea CE al BNM nr. 281 din 07.11.2024, Regulamentul privind cerințele pentru identificarea și verificarea identității clienților prin intermediul mijloacelor electronice** [NBM e-KYC Regulation], points 5 to 52, MO 467-469/14.11.2024, legis.md
- **Hotărârea CE al BNM nr. 200 din 09.08.2018, Regulamentul cu privire la cerințele privind prevenirea și combaterea spălării banilor și finanțării terorismului în activitatea băncilor** [NBM AML/CFT Regulation for banks], points 25, 26, 38, 39, 55, 57^1, 59, last amended by Decision No. 8 of 13.01.2025, legis.md
- **NBM, announcement of public consultation on amending the e-KYC Regulation**, 16 February 2026 (deadline 2 March 2026), with draft decision, bnm.md
- **NBM, Sancțiunile aplicate de Banca Națională a Moldovei în temeiul Legii privind activitatea băncilor** [sanctions table], decisions No. 67 of 19.03.2026 and No. 216 of 09.09.2026, bnm.md
- **Legea nr. 195 din 25.07.2024 privind protecția datelor cu caracter personal** [Law No. 195/2024 on personal data protection], arts. 9, 88, 89, 90, last amended by Law No. 160/2026, legis.md
- **Legea nr. 25 din 04.03.2016 privind aplicarea măsurilor restrictive internaționale** [Law No. 25/2016 on international restrictive measures], arts. 6(6) and 28(1), last amended by Law No. 244/2025, legis.md
- **Legea nr. 180 din 24.08.2026 privind piața criptoactivelor** [Law No. 180/2026 on the crypto-asset market], arts. 17, 45, 53, 54, 104 (version in force from 17.03.2027), MO 456-459/17.09.2026, legis.md
- **Legea nr. 66 din 30.03.2023 pentru modificarea unor acte normative** [Law No. 66/2023 amending Law 308/2017], art. I (art. 5(4^1)-(4^4) of Law 308), MO 159-161/11.05.2023, legis.md
- **Legea nr. 114 din 18.05.2012 cu privire la serviciile de plată şi moneda electronică** [Law No. 114/2012 on payment services and electronic money], arts. 5, 52^4, legis.md

- **Hotărârea CE al BNM nr. 12 din 11.01.2024, Regulamentul cu privire la autentificarea strictă a clienților și standardul deschis, comun și sigur de comunicare** [NBM Regulation on strong customer authentication], points 18, 19, 31, last amended by Decision No. 267 of 31.10.2024, legis.md
- **Hotărârea CE al BNM nr. 46 din 26.02.2020, Regulamentul privind externalizarea activităților și operațiunilor băncii** [NBM Regulation on outsourcing by banks], points 6, 38, last amended by Decision No. 29 of 12.02.2025, legis.md
- **Hotărârea CNPF nr. 63/1 din 19.12.2023, Regulamentul privind măsurile de prevenire și combatere a spălării banilor și finanțării terorismului** [CNPF AML Regulation], point 59, MO 28-31/23.01.2024, legis.md
- **SPCSB, Consultări publice asupra proiectelor de lege în domeniul prevenirii și combaterii spălării banilor** [public consultation on draft AML laws], 28 October 2026, spcsb.md; draft AML law (No. 864/SPCSB, arts. 22, 124) and consultation stages (26.10.2026 to 02.11.2026), particip.gov.md; draft law on the procedure for AML breaches and sanctions (No. 865/SPCSB/2026, art. 26(4)), particip.gov.md
- **SPCSB, Formare profesională** [national AML training course, examination and certificate], spcsb.md
- **SPCSB, Deschiderea unui cont pentru altcineva te poate transforma în complice la infracțiuni** [notice on money mule accounts], 10 June 2026, spcsb.md
- **CNPF, Anunț privind inițierea elaborării proiectului Regulamentului privind notificarea intenției de a furniza servicii de criptoactive** [notice of drafting], 21 October 2026, cnpf.md
- **MONEYVAL, Republic of Moldova** [evaluation and follow-up reports], Council of Europe, coe.int