Identomat

COMPLIANCE GUIDE

Crypto & Virtual Assets Compliance in Armenia

COUNTRY Armenia

INDUSTRY Crypto & Virtual Assets

LAST UPDATED 13 November 2026

KEY REGULATORS Central Bank of Armenia · Financial Monitoring Center

Key takeaways

- Crypto exchanges, brokers, custodians, transfer services and issuers of asset-referenced tokens serving customers in Armenia need a licence from the Central Bank of Armenia (CBA); investment firms and some other existing institutions need a CBA authorisation instead. Foreign firms can only operate through an Armenian subsidiary or branch.
- Companies that were already operating on 4 July 2025 have until 31 January 2027 to obtain a licence or stop offering crypto services in Armenia.
- Online onboarding is allowed, but a customer you never meet in person counts as high risk by default. The first payment must also come from an account in the customer's own name at a regulated financial institution.
- The Travel Rule (the duty to send sender and recipient details with each transfer) applies to every crypto transfer, with no minimum amount. A firm must refuse to send a transfer without the required details and needs risk-based procedures for incoming transfers that lack them.
- Crypto transactions of AMD 1 million or more must be reported to the Financial Monitoring Center (FMC), Armenia's financial intelligence unit, whatever the channel. Suspicious activity is reported at any amount.

Armenia is open to crypto businesses, but only under a licensing regime that the Law on Crypto-assets introduced in July 2025 and that the CBA's first implementing regulations put into operation on 31 January 2026. The CBA is the single authority: it licenses and supervises crypto-asset service providers, and the FMC within the CBA receives their anti-money laundering reports.

The biggest obstacle for a new entrant is establishment. A licence goes only to an Armenian joint-stock or limited liability company whose business is limited to crypto services, with head office premises in Armenia, registered managers, approved qualifying shareholders and minimum capital of AMD 10 million to AMD 200 million depending on the service.

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
Central Bank of Armenia (CBA)	Licensing and supervision of crypto-asset service providers, public offers of crypto-assets and asset-referenced tokens; sanctions under the Law on Crypto-assets	National	cba.am
Financial Monitoring Center (FMC), a separate unit of the CBA	Financial intelligence unit: receives suspicious and threshold reports and publishes guidance and sanctions lists (the CBA itself is the "authorised body" under the anti-money laundering law, art. 3(1)(7))	National	cba.am
Personal Data Protection Agency of the Ministry of Justice	Authorised body for personal data, acting independently (Law on Protection of Personal Data, art. 24(2)); receives mandatory notice before biometric processing (art. 23(3))	National	moj.gov.am
MONEYVAL (Council of Europe)	Evaluates Armenia's anti-money laundering regime against the FATF Recommendations	Supranational	coe.int

Tax treatment of crypto-assets and the State Revenue Committee's role fall outside this guide.

2 Licensing and authorisation

The Law of the Republic of Armenia on Crypto-assets (HO-159-N, adopted 29 May 2025, in force 4 July 2025, last amended by HO-515-N of 17 December 2025) `In force` prohibits offering or providing any of the ten crypto-asset services listed in art. 16, directly or indirectly, without a CBA licence (art. 17(1)).

Who can hold a licence

- **Crypto-asset service provider:** an Armenian joint-stock or limited liability company licensed by the CBA Board, limited to crypto services and closely related activities the CBA allows (art. 17(2), (5), (6)); the licence is indefinite, service-specific and non-transferable (art. 19).
- **Existing financial institutions:** investment companies, fund managers, a regulated market operator and the Central Depository need a CBA authorisation (art. 18).
- **Foreign providers:** only through an Armenian subsidiary or branch (art. 21).
- **Stablecoins:** asset-referenced tokens need the issuance licence; dram-pegged electronic money tokens may be issued only by banks and electronic money issuers (arts. 59, 68).

Process, capital and premises

Applications include internal rules, a business plan (for platforms, custody and token issuance), manager registrations, qualifying-holding approvals, proof of paid-in capital and declarations on premises and information security (art. 20(1)). The CBA Board decides within two months (art. 20(8)). CBA Regulation 7/01 and Regulation 7/05 (managers), in force since 31 January 2026, set the procedure; head office premises must be in Armenia (7/01, pt 90).

Minimum total capital under CBA Regulation 7/02 (pts 7 and 8) is the highest of a fixed amount per service, 25% of fixed overheads and, for token issuers, 2% (3% with 50,000 or more holders) of average reserve assets:

Service	Fixed minimum capital
Advice on crypto-assets	AMD 10 million
Execution for clients, reception and transmission of orders, placement, portfolio management, transfer	AMD 20 million

Dealing on own account, custody	AMD 50 million
Operating a trading platform	AMD 70 million
Issuing asset-referenced tokens	AMD 200 million

Transition for existing providers

Legal entities providing crypto services on 4 July 2025 must be licensed by 31 January 2027 (one year after Regulation 7/01 took effect) or stop; sole traders must stop then (art. 94(2)). Providers that notified the CBA before 31 January 2026 sit on a transitional list; others may deal only by non-cash payment (art. 94(2.1) to (2.4)).

3 AML, KYC and customer due diligence

Under the Law on Combating Money Laundering and Terrorism Financing (HO-80-N of 2008, crypto provisions added by HO-180-N, in force 4 July 2025), crypto-asset service providers are reporting entities and financial institutions, except providers of trading platform operation services (art. 3(1)(4)(i1) and (5)); MONEYVAL's 2026 report records the same carve-out. Platform rules must still bar trading in crypto-assets that keep the parties anonymous, unless the operator can identify acquirers and their transaction history (Law on Crypto-assets, art. 51(4)). The detailed rules are in the CBA's Regulation on Minimum Requirements to Reporting Entities (Board Decision 279-N, amended by Decision 11-N of 22 January 2026, in force 30 January 2026).

When CDD applies

On establishing a business relationship; on occasional transactions, including linked ones within 24 hours and crypto-asset transfers, of 400 times the minimum wage or more (AMD 400,000, as laws use AMD 1,000 as the calculation base); on doubts about identification data; and on any suspicion (art. 16(2)).

Beneficial ownership

A natural person holding 20% or more of voting shares or charter capital, directly or indirectly, or exercising control by other means; a senior manager as fallback (art. 3(1)(14)). Steps and conclusions must be documented (art. 16(5.1)).

Enhanced due diligence

Required whenever a high-risk criterion is present (art. 18(2)); risk is high if any criterion applies (Regulation pt 23), and where criteria for different levels coexist the highest governs (pt 25). Criteria include non-face-to-face relationships, politically exposed persons, persons from non-compliant jurisdictions and complex or unusually large transactions (pt 27).

Reliance

A firm may rely on CDD by another regulated institution, but keeps ultimate responsibility and must obtain the data immediately (art. 16(8)).

Reporting and records

- **Suspicious transactions:** reported to the FMC at any amount, including attempts (arts. 6(2) and 7). The CBA sets report forms and deadlines by type of reporting entity (art. 8(5)); as of November 2026 none has been adopted for crypto-asset service providers.
- **Threshold reports for financial institutions** (art. 6(3)(1)): crypto-asset transactions of AMD 1 million or more; cash-related transactions of AMD 5 million or more; non-cash transactions of AMD 20 million or more.
- **Ongoing CDD:** identification and verification data must be refreshed at least once a year (art. 17(2)); other CDD information yearly at standard risk and six-monthly at high risk (pt 38), with transaction monitoring on the same cycle (pt 37) and politically exposed persons reviewed at least every three months (pt 41). Other periods need a documented analysis submitted to the CBA (pt 41.1).
- **Retention:** CDD data and records for at least five years after the relationship ends or the transaction is completed (art. 22(2)); risk assessments for at least five years (art. 4(6)).

4 Identity verification and onboarding

Customers are identified and verified on the basis of reliable and valid documents and other information issued by a competent state body (art. 16(4)). For an individual, the firm must record at least name, citizenship, registration address (if any), date and place of birth, and the series, number and issue date of the identity document, and must establish the place of residence. Legal entities provide registration data, charter and manager details.

Verification of the customer, any representative and the beneficial owner may follow onboarding by up to seven days, if the risk is effectively managed and delay is needed not to disrupt normal business (art. 16(1)). The firm's policy must say which transactions, of what number or value, the customer may carry out before verification (art. 18(3.1)).

Neither the law nor the CBA regulation names a remote method (video identification, liveness, chip reading) or an identity assurance level.

Outsourcing. Delegating any function other than a supporting function needs the CBA's prior consent, or the contract is void, and the provider keeps final liability (Law on Crypto-assets, art. 43(4) and (5)). CBA draft Regulation 7/13 `Draft` would limit supporting functions to administrative tasks such as staff, legal, payroll and tax, so using an outside identity verification provider should be checked against this rule.

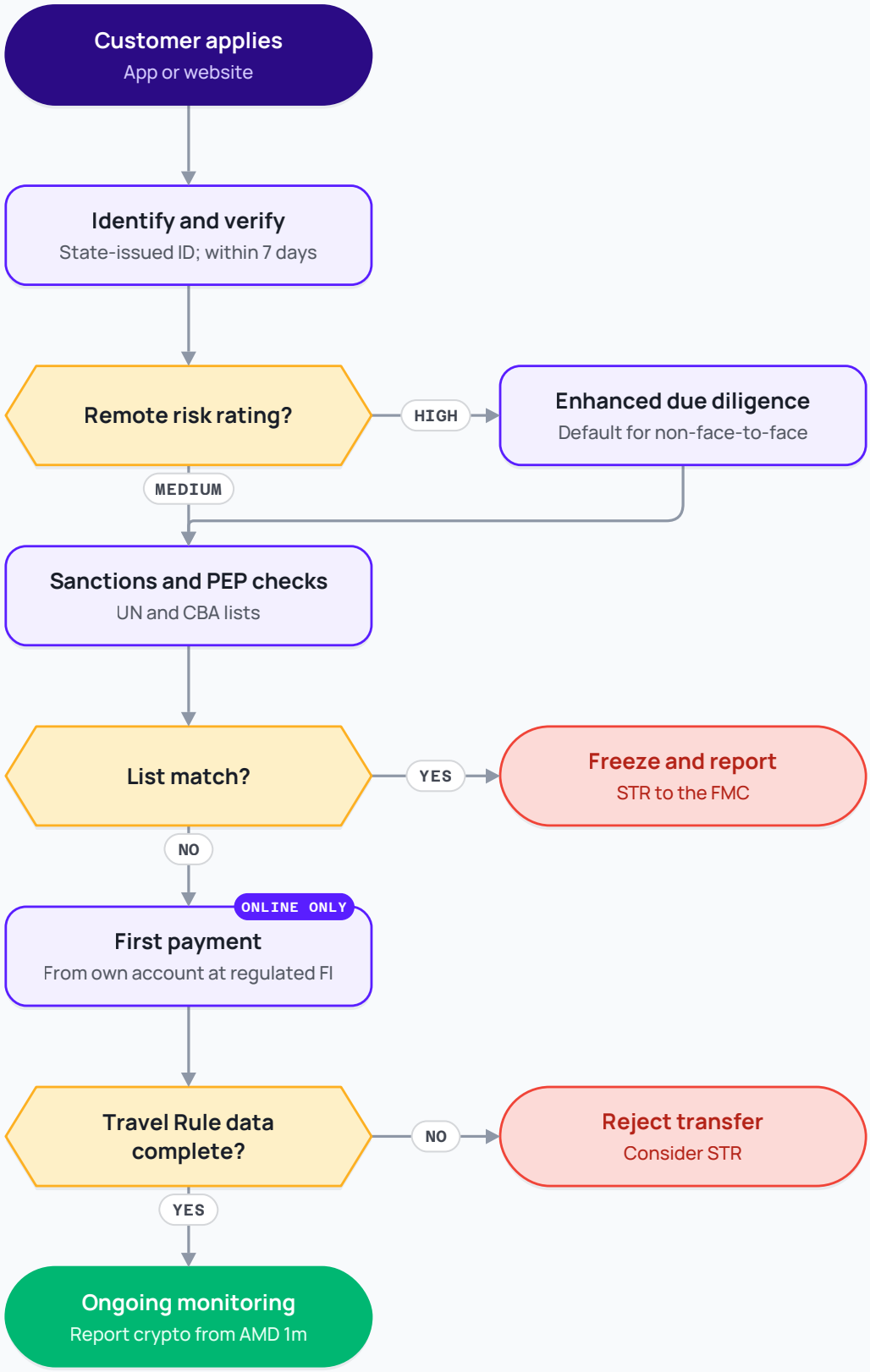


Figure 1. Remote onboarding and first transfer at an Armenian crypto-asset service provider.

5 Digital channels: what's different

Bottom line: the same licence and identification data apply in every channel, but a customer onboarded remotely is high risk by default and must make the first payment from an account in their own name at a regulated financial institution.

Requirement	In person / land-based	Online / remote	Difference
Licence	CBA licence; head office in Armenia	Same licence; foreign online providers need an Armenian subsidiary or branch	Same
Identification data	State-issued document; set data list	Same data list; no remote method prescribed	Same
Verification timing	At onboarding, or within 7 days	At onboarding, or within 7 days	Same
Risk rating	Standard unless other criteria apply	High-risk criterion; medium only with a documented analysis submitted to the CBA	Differs
First payment	No specific rule	From an account in the customer's name at a regulated institution	Differs
Payment form	Cash up to AMD 300,000 via an identifying provider (until 1 Jan 2028)	Non-cash	Differs
Customer location	Not applicable	IP address in a non-compliant country is a CBA suspicion indicator	Differs
Travel Rule	All crypto transfers, no threshold	All crypto transfers, no threshold	Same
Threshold reporting	Crypto from AMD 1 million	Crypto from AMD 1 million	Same

Non-face-to-face is a high-risk criterion

The CBA regulation lists a relationship without face-to-face contact as a high-risk criterion (pt 27(6)), and one high-risk criterion makes the relationship high risk (pt 23). A firm may rate it medium only after a comprehensive, documented analysis concluding that the risks are effectively managed, submitted to the CBA as authorised body (pt 22.1). The law also requires specific identification and verification procedures for such relationships (art. 18(3)).

First payment from a verified account

When a business relationship is established without face-to-face contact, the firm must require the first payment to come from an account opened in the customer's name at a financial institution that is itself regulated and supervised for anti-money laundering purposes and not based in a non-compliant jurisdiction (pt 40, referring to art. 16(8)(3)).

Cash belongs to the counter, not the app

Payment for crypto-assets and for crypto-asset services in Armenia must be non-cash (Law on Non-cash Transactions, art. 6.1(1) and (2)). Until 1 January 2028 a cash purchase of up to AMD 300,000 is allowed only through a licensed or transitional-list provider that identifies the customer and records the transaction (art. 6.1(3); Law on Crypto-assets, art. 94(2.1)). Transitional-list providers must video-record service premises and crypto ATMs with the customer's face visible, keep footage six months, and keep identity document copies five years (CBA Board Decision 12-N of 26 January 2026, pts 4, 9, 10 and 12).

6 Data protection and biometrics

Under the Law on Protection of Personal Data («Անձնական տվյալների պաշտպանության մասին»), biometric data may be processed only with consent, unless a law provides otherwise (art. 13). The AML law does not mandate biometrics, so face matching or liveness rests on consent. Consent must be in writing, or electronic and certified with an electronic digital signature; oral consent counts only through reliable actions that clearly show it (art. 9(7)), so a tick-box alone may not meet this. Before processing biometric data the firm must notify the Personal Data Protection Agency (art. 23(3)). Identity records are kept five years (AML law, art. 22(2)).

7 Sector-specific obligations

Travel Rule for crypto transfers

Sending and receiving institutions must obtain and keep originator and beneficiary names, their ledger addresses or crypto-asset account numbers, and identity document data, address, or date and place of birth (AML law, art. 20.1(1)). The sender passes the data immediately and securely, possibly off-chain, with no minimum amount (art. 20.1(2)). Incomplete incoming transfers need risk-based procedures (art. 20.1(5)); outgoing requests missing the data must be refused (art. 27(4)). The law sets no separate procedure for self-hosted wallets, but the CBA's risk guideline (section 8) makes funds from decentralised wallets or trading platforms a high-risk criterion (pt 1.2.3.6).

Sanctions and freezing

Property of persons designated by the UN Security Council or on CBA-published lists must be frozen immediately and without notice (AML law, art. 28). The CBA's freezing guidance (2018) requires screening customers and counterparties against the lists, including with the cba.am search tool, and on a match a freeze and a suspicious transaction report (pt 8).

Custody, tokens and records

Custody, platforms and token issuance carry their own rules (arts. 51 to 68). Transitional-list providers record every transaction, including at crypto ATMs (Decision 12-N). Draft Regulation 7/07 would require at least 50% of custody in cold wallets and segregated client assets (pts 90, 92).

8 Risk indicators and red flags

The CBA's Guideline on the Criteria of High Risk and the Indicators of Suspicious Activity in Relation to Money Laundering and Terrorist Financing (published by the FMC; amended by CBA Chairman's Decision 1/347-A of 24 September 2025) lists crypto-asset service providers among cash- and crypto-intensive businesses and sets crypto-specific indicators:

CRYPTO-ASSET INDICATORS (CBA GUIDELINE)

- **Unregistered platforms**: funds come from or go to a platform not registered in the country of the customer or the provider (2.2.2.64).
- **Terrorism-linked addresses**: funds linked, directly or indirectly, to a wallet address recognised as suspicious for terrorism or its financing (2.2.2.66).
- **Non-compliant jurisdictions**: crypto-assets sent to platforms in non-compliant countries or without effective supervision (2.2.2.67).
- **Linked wallets**: transactions between accounts or wallets opened by persons connected by common data, such as citizenship or IP address (2.2.2.69).
- **Mixers and privacy coins**: use of mixers or tumblers, or funds from the sale of privacy coins (2.2.2.70).
- **Cross-chain bridges**: frequent or high-value deposits or withdrawals through bridges (2.2.2.71).
- **Instant-payment inflows**: a customer providing crypto services receives large amounts through fast or instant transfer systems (2.2.2.68).
- **Decentralised sources**: funds obtained from decentralised wallets or trading platforms, a high-risk criterion (1.2.3.6).

9 Enforcement and penalties

AML breaches by crypto-asset service providers are sanctioned under the Law on Crypto-assets (AML law, art. 30(2)). The CBA may warn, fine, deregister a manager, revoke a licence or end an authorisation, combining sanctions (art. 83(1)-(2)). It may also suspend specific services, offers or trading for up to six months (art. 83(5)).

Fines are set by the CBA Governor (art. 85):

- up to 300% of the profit or loss generated by the breach, where it can be measured;
- otherwise, for legal persons, up to 15% of annual revenue or income based on the last audited financial statements;
- for natural persons, up to 20,000 times the minimum wage (AMD 20 million at the AMD 1,000 calculation base).

No sanction against a crypto-asset service provider appears on the CBA's sanctions page (as of November 2026). On 24 November 2025 the CBA warned the public that "DaoBit",

"Orbis" (Orbis Exchange) and "GKGD" were offering high returns without any CBA licence and outside its supervision. MONEYVAL found no licensed provider at its October 2025 visit.

10 Recent changes and what to watch

- **31 January 2027:** `Deadline for existing providers` Unlicensed providers that were operating on 4 July 2025 must stop offering crypto services.
- **16 October 2026:** `Draft, consultation closed 30 Oct 2026` CBA draft extending its information security minimums (Decision 173-N) to platforms, custodians, order execution and transmission, and token issuers.
- **12 August 2026:** `Draft, consultation closed 26 Aug 2026` CBA draft Regulation 7/07 (conduct, cash desks, at least 50% of custody in cold wallets) and amendments to Decision 12-N (reporting by licensed providers; crypto ATM notices).
- **9 July 2026:** `Published` MONEYVAL's report (adopted at the 71st Plenary, 27-29 May 2026) rates Armenia largely compliant on new technologies (R.15), calls for stronger supervision of providers, and puts Armenia in enhanced follow-up.
- **31 January 2026:** `In force` CBA Regulations 7/01 (licensing), 7/02 (capital), 7/04 (white papers) and 7/05 (managers) took effect.
- **17 December 2025:** `In force` Law HO-515-N created the CBA transitional list and the non-cash rule for providers not on it; Law HO-516-N keeps the cash exception for purchases up to AMD 300,000 until 1 January 2028.
- **24 September 2025:** `In force` CBA guideline adds crypto-asset indicators.

11 What this means for identity verification

- **Documents:** capture the full data list from a state-issued identity document, plus place of residence; for foreign customers, also record the centre of vital interests (AML law, art. 18(4)).
- **Remote methods:** none is prescribed, so the firm's non-face-to-face policy must justify its choice.
- **Risk engine:** default remote customers to high risk, or keep a documented analysis, submitted to the CBA, that supports a medium rating.
- **Re-verification:** refresh identification and verification data at least once a year (art. 17(2)), and repeat CDD when identification data is in doubt (art. 16(2)(3)) or a new risk criterion appears (pt 26).

- **Funding check:** match the first funding account's name to the verified customer.
- **Biometrics:** capture consent in a form that meets art. 9(7) and notify the Agency before processing (art. 23(3)).
- **Vendors:** check whether an outside verification provider needs CBA delegation consent.
- **Signals:** capture IP address and wallet provenance (CBA risk indicators).
- **Transfers:** send Travel Rule data with every transfer; refuse incomplete outgoing requests and handle incomplete incoming ones by risk.

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 identity verification against state-issued ID documents, capturing the full data set the anti-money laundering law requires, with face match and liveness detection.
- Configurable risk-based workflows that flag non-face-to-face onboarding for enhanced due diligence and keep an audit trail for each check.
- Screening against sanctions, PEP and watchlists at onboarding and on an ongoing basis, supporting immediate freezing decisions.
- KYB and beneficial owner verification for corporate clients at the 20% ownership threshold.
- Consent capture with e-signatures before biometric checks, and cloud, on-premises or hybrid deployment to fit data residency needs.

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

- «**Կրիպտոակտիվների մասին» ՀՀ օրենք** [Law of the Republic of Armenia on Crypto-assets], **HO-159-N of 29 May 2025, as amended by HO-515-N of 17 December 2025**, ARLIS, arlis.am (Armenian); official English translation, arlis.am (English)
- «**Փողերի լվացման և ահաբեկչության ֆինանսավորման դեմ պայքարի մասին» ՀՀ օրենք** [Law on Combating Money Laundering and Terrorism Financing], **HO-80-N of 26 May 2008, as amended**, arts. 3, 4, 6, 7, 8, 16, 18, 20.1, 22, 27, 28, 30, ARLIS, arlis.am
- **Law HO-180-N of 29 May 2025 amending the Law on Combating Money Laundering and Terrorism Financing** (in force 4 July 2025), ARLIS, arlis.am
- **CBA Board Decision 279-N of 7 October 2014, Regulation on Minimum Requirements to Reporting Entities in the Field of Preventing Money Laundering and Terrorism Financing**, as amended by Decision 11-N of 22 January 2026 (in force 30 January 2026), pts 22.1, 23, 25, 26, 27, 37, 38, 40, 41, 41.1, ARLIS, arlis.am
- **CBA Board Decision 227-N of 30 December 2025, Regulation 7/01 on the registration and licensing of crypto-asset service providers** (in force 31 January 2026), official English translation, ARLIS, arlis.am
- **CBA Board Decision 228-N of 30 December 2025, Regulation 7/02 on minimum thresholds for the total capital of crypto-asset service providers** (in force 31 January 2026), pts 7 and 8, ARLIS, arlis.am
- **CBA Board Decision 226-N of 30 December 2025, Regulation 7/04 on crypto-asset white papers**, official English translation, ARLIS, arlis.am
- **CBA Board Decision 229-N of 30 December 2025, Regulation 7/05 on registration of executive officers of crypto-asset service providers**, official English translation, ARLIS, arlis.am
- **CBA Board Decision 12-N of 26 January 2026 on records of crypto-asset transactions and their submission to the Central Bank** (in force 30 January 2026), ARLIS, arlis.am
- «**Անկանխիկ գործառնությունների մասին» ՀՀ օրենք** [Law on Non-cash Transactions], **HO-12-N of 18 January 2022**, art. 6.1, ARLIS, arlis.am
- «**Նվազագույն ամսական աշխատավարձի մասին» ՀՀ օրենք** [Law on Minimum Monthly Wage], **HO-66-N of 17 December 2003**, art. 3, ARLIS, arlis.am
- «**Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենք** [Law on Protection of Personal Data], **HO-49-N of 18 May 2015**, arts. 9(7), 13, 23(3) and 24(2), official English title on ARLIS, arlis.am (English); current Armenian text, arlis.am
- **Central Bank of Armenia, Crypto-asset service providers** (licensing requirements, transition deadline, draft regulations), cba.am; list of providers under art. 6.1(3) of the Law on Non-cash Transactions, cba.am
- **CBA draft Regulation 7/07, Rules and requirements for the activities of crypto-asset service providers**, pts 90 and 92, cba.am (PDF); CBA draft decision amending Board Decision 12-N, cba.am (PDF); CBA announcement of public consultation, 12 August 2026 (comments until 26 August 2026), cba.am

- **CBA draft decision amending Board Decision 173-N on minimum information security requirements**, cba.am (PDF); CBA announcement, 16 October 2026 (comments until 30 October 2026), cba.am
- **CBA draft Regulation 7/13 on prior consent for delegation of functions by crypto-asset service providers**, cba.am (PDF)
- **CBA, Reminder to crypto-asset service providers**, 14 September 2026, cba.am
- **CBA, Warning about "DaoBit", "Orbis" and "GKGD"**, 24 November 2025, cba.am
- **CBA (published by the FMC), Guideline on the Criteria of High Risk and the Indicators of Suspicious Activity in Relation to Money Laundering and Terrorist Financing**, annex to CBA Chairman's Decision 1/711-A of 11 October 2016 as amended by Decision 1/347-A of 24 September 2025, pts 1.2.1.8, 1.2.3.6, 2.2.2.59 and 2.2.2.64 to 2.2.2.71, cba.am (PDF, English)
- **Government Decision 734-N of 2 July 2015 establishing the Personal Data Protection Agency of the Ministry of Justice**, ARLIS, arlis.am; Ministry of Justice, Structure (Agencies of the Ministry), moj.gov.am
- **CBA (published by the FMC), Guidance on freezing of property of persons and entities related to terrorism or proliferation of weapons of mass destruction, providing access to frozen property and related actions**, approved by CBA Chairman's Order 1/435-A of 26 June 2018, pt 8, cba.am (PDF, English)
- **MONEYVAL, Armenia: Sixth Round Mutual Evaluation Report, May 2026** (MONEYVAL(2026)8), adopted at the 71st Plenary (27-29 May 2026), published 9 July 2026, R.15 (criteria 15.6 and 15.9), rm.coe.int; Executive Summary (ratings), rm.coe.int
- **MONEYVAL, "Armenia: Council of Europe's MONEYVAL highlights robust targeted financial sanctions regime, calls for improvements in money-laundering prosecutions and asset recovery"**, 9 July 2026, coe.int