Identomat

COMPLIANCE GUIDE

Crypto & Virtual Assets Compliance in Azerbaijan

COUNTRY Azerbaijan

INDUSTRY Crypto & Virtual Assets

LAST UPDATED 13 November 2026

KEY REGULATORS Central Bank of the Republic of Azerbaijan · Financial Monitoring Service

Key takeaways

- Azerbaijan has no licence or registration for crypto businesses (as of November 2026). The only official channel is the regulatory sandbox of the Central Bank of the Republic of Azerbaijan (CBAR), a time-limited test with a licence exemption, in which five crypto products have been tested since November 2024.
- The anti-money laundering (AML) law already treats virtual asset service providers (VASPs) as financial institutions supervised by CBAR, so customer checks, reporting and record-keeping apply now.
- CBAR's Travel Rule (sending sender and recipient details with each transfer) is adopted but takes effect only once a law regulating VASPs is passed.
- Online onboarding is allowed but treated as higher risk. A first remote relationship needs an strengthened electronic signature, a database check, two-factor authentication and a live video call or recording. Non-resident companies cannot be onboarded remotely.
- Fines for financial institutions reach AZN 30,000 per customer or transaction for due diligence failures and AZN 50,000 per person for failing to freeze sanctioned assets. Reporting rules change on 1 January 2027.

The market is unregulated at the entry point: no statute licenses VASPs, and CBAR's virtual asset rules state that services are provided by VASPs permitted to do so by law. Firms can seek a place in CBAR's regulatory sandbox or wait for a VASP law, while AML duties already apply.

CBAR supervises VASPs for AML purposes and runs the sandbox; the Financial Monitoring Service (FMS), the financial intelligence unit, sets the detailed due diligence rules and receives reports.

The biggest obstacle for a new entrant is legal uncertainty, combined with a strict remote onboarding regime that requires live video identification.

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 crypto businesses	Level	Official site
Central Bank of the Republic of Azerbaijan (CBAR)	AML supervisor of all financial institutions, including VASPs; issues the virtual asset rules; runs the regulatory sandbox	National	cbar.az
Financial Monitoring Service (FMS)	Financial intelligence unit; sets due diligence, risk and remote verification rules and reporting thresholds; receives reports	National	fiu.gov.az
Ministry of Digital Development and Transport	Authority for personal data, including biometric data	National	mincom.gov.az
MONEYVAL (Council of Europe)	Evaluates Azerbaijan's AML and counter-terrorist financing regime, including the standard on virtual assets	Supranational	coe.int/moneyval

2 Licensing and authorisation

No law provides a licence, registration or authorisation for VASPs. The Law on the Prevention of the Legalization of Criminally Obtained Property and the Financing of Terrorism (No 781-VIQ of 30 December 2022, the AML/CFT Law) defines a VASP by activity: exchanging virtual assets for currency or other virtual assets; transferring them between

accounts or wallets; organising transactions in, or safekeeping of, virtual assets; and financial services linked to their purchase, sale, exchange, initial placement or custody, carried out as an independent business (art. 1.1.12). Digital equivalents of currency, securities and derivatives are not virtual assets (art. 1.1.11).

CBAR Management Board Decision No 11/1 of 24 February 2023 approved the Rule for conducting operations with virtual assets in the Republic of Azerbaijan `Adopted, effective date not yet set`. Point 2 of the decision states that the Rule enters into force only after normative legal acts regulating VASP activity are adopted; no such law has been adopted as of 13 November 2026.

The regulatory sandbox

Under article 50 of the Law on the Central Bank (No 802-IIQ), CBAR may let innovative financial products be tested on a limited scale under its supervision. Its Rule on the application of the special regulatory regime (Decision No 06/4 of 31 January 2024) exempts participants from licensing requirements (point 3.2.1). Applicants must be legal entities registered in Azerbaijan whose owners and managers meet the AML/CFT Law's integrity tests (no relevant criminal convictions, art. 17.2), and the product must not increase money laundering or terrorist financing opportunities (points 2.1.4, 3.1.4, 3.1.6). Applications are accepted only in windows announced at least a month in advance; CBAR normally decides within 20 working days; a test runs for up to 12 months, extendable by up to 6 months at a time within an overall 5-year limit; users must be told in writing that the product is in a test (points 4.1, 5.1, 6.4, 9.2). The public sandbox registry shows five crypto products tested since November 2024: three tests (transfers to a crypto exchange wallet, a crypto trading platform and a crypto token) have ended, and a crypto broker and a crypto exchange are still listed as current.

3 AML, KYC and customer due diligence

VASPs are financial institutions under the AML/CFT Law (art. 1.1.8) and CBAR is their supervisor (art. 16.1.1). The AML/CFT Law applies from 1 February 2023 (art. 25.2).

When CDD applies

Before a business relationship; before occasional transactions of AZN 20,000 or more, including linked transactions; before occasional virtual asset transactions under CBAR rules; on any suspicion; and when earlier data is doubtful (art. 4.2).

What CDD covers

Identify and verify the customer and any representative from reliable independent sources, identify the beneficial owner, establish the purpose of the relationship and build a customer profile (art. 4.4). If CDD cannot be completed, do not transact and report to the FMS (art. 4.14).

Enhanced due diligence

Required where risk is high, for politically exposed persons (PEPs) with management approval and source-of-wealth checks (art. 7.1), and for customers linked to high-risk zones (art. 9.1). Relationships created through new technologies are treated as high risk (art. 8.1).

Ongoing monitoring

CDD data is refreshed at least annually for high-risk customers, every two years for medium risk, every three years for low risk, and continuously for PEPs (FMS Rules, point 8.1).

Beneficial ownership

For a legal entity, identify the natural persons with a significant participation (10% or more), then anyone controlling it by other means, then senior management (AML/CFT Law arts. 1.1.20, 4.7). Beneficial owner data on corporate customers goes to the FMS within 3 working days (art. 11.11).

Reporting thresholds

Under the FMS reporting decision of 27 April 2023 (No 3-21-28/3-6-8/2023):

- **Cash transactions** of AZN 20,000 or more: report within 3 working days (AML/CFT Law arts. 11.1.1, 11.4).
- **Electronic transfers** of AZN 20,000 or more, expressly including transfers between a bank account and a virtual asset account or wallet: report within 3 working days (art. 11.1.2).
- **Suspicious transactions and attempts**, at any amount (art. 11.2).
- **Suspicious transactions of AZN 200,000 or more**, linked to a high-risk profile, or withdrawing funds: do not execute for 2 working days and report first (art. 11.5).
- **Any transaction** by a foreign PEP, and transactions with sanctioned persons' assets, regardless of amount (art. 11.3).

From 1 January 2027 `Adopted, effective 1 Jan 2027`, FMS Decision No 3-21-28/3-6-7/2026, as amended by FMS Decision No 3-21-28/3-6-17/2026 (which moved the start from 1 October 2026), adds a monthly tier: once an individual's (other than a sole proprietor's) transfers exceed AZN 50,000 in a calendar month, each further transfer is reported. Reports go through the FMS "Suspicious transactions monitoring" information system, and where the merchant in a reported payment is a VASP, the report carries the name on the virtual asset account and its identifiers. Customers must not be told about a report (art. 11.10), and records are kept for at least 5 years (art. 6).

4 Identity verification and onboarding

The FMS Rules on verification measures, identification of risk factors and attribution of the customer profile to risk groups during the application of customer compliance and new technologies (Decision No 3-21-28/3-6-4/2023 of 21 February 2023, the FMS Rules) set the data and evidence required.

Data and documents

For individuals, firms collect full name, personal identification number (FİN) or document number, citizenship, residency, date of birth, contact details, employment, income sources, purpose of the relationship and expected volumes (point 2.1.1). Identity is verified against an accepted document (point 6.1.1.1): the national identity card for citizens; a foreign passport or residence permit for foreign nationals; and specified documents for stateless persons, refugees, military personnel and seafarers (Annex).

Remote onboarding

For a **first** remote business relationship, four measures are mandatory (point 7.2):

- confirmation of the application with the customer's strengthened electronic signature;
- checking the customer's data against electronic databases or independent sources;
- strong customer authentication using two or more independent factors of knowledge, possession and inherence (face recognition, voice or fingerprint are given as examples);
- identity verification through a real-time video call or a video recording made through the system.

A strengthened electronic signature (gücləndirilmiş elektron imza) is one under the signatory's sole control that identifies them and reveals any alteration (Law on Electronic Signature and Electronic Document, No 602-IIQ, art. 1.1.5); backed by a complete certificate

(təkmil sertifikat) from an accredited centre, it equals a handwritten signature (art. 3.2). The State Tax Service describes ASAN İmza, the mobile signature issued by the ASAN Certification Services Center of the State Tax Service with the mobile operators, as an strengthened electronic signature.

If identity cannot be established remotely, the firm must refuse to proceed remotely (point 7.3). Remote onboarding through an authorised representative (other than a company's legal representative) and of non-resident legal entities is not permitted (point 7.4). Verification may finish after the relationship starts, within 5 working days, if the firm limits transactions meanwhile (points 6.4.1, 6.5).

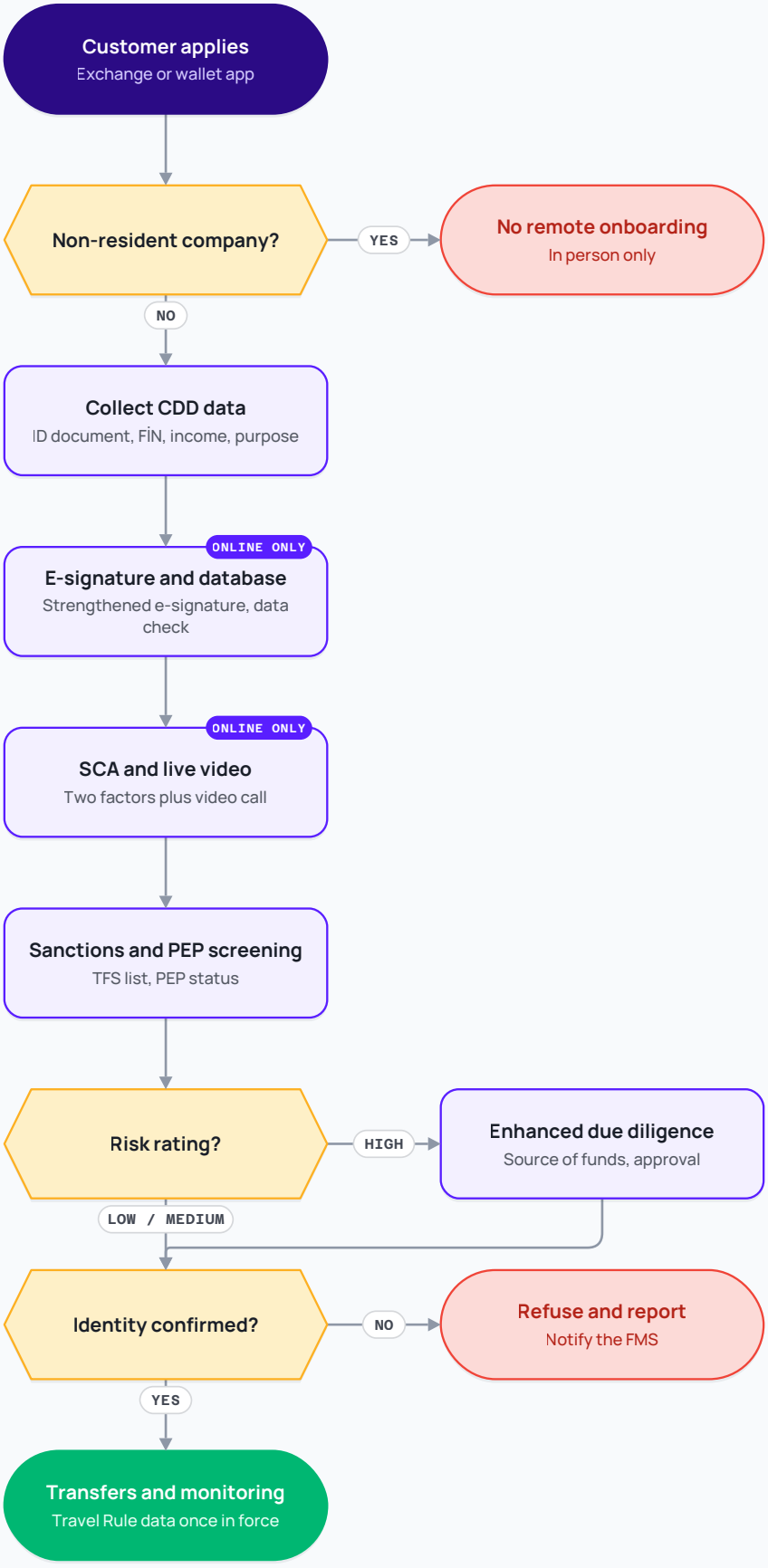


Figure 1. Remote onboarding of an individual customer by a virtual asset service provider in Azerbaijan.

5 Digital channels: what's different

Bottom line: remote onboarding is lawful but classed as high risk, and a first remote relationship requires an strengthened electronic signature, a database check, two-factor authentication and live video identification together.

Requirement	In person	Online / remote	Difference
Channel risk	Face-to-face channels may be rated low risk	Non-face-to-face and new-technology channels treated as high risk	Differs
Identity verification	Accepted identity document	Four mandatory measures incl. live video for a first relationship	Differs
Timing of verification	Before the relationship	May finish within 5 working days, with usage limits	Differs
Representatives and non-resident companies	Permitted	Not permitted remotely	Differs
Accepted identity documents	Listed in the FMS Rules annex	Same list	Same
Reliance on another obliged entity	Allowed, liability retained	Allowed, liability retained	Same
Reporting thresholds	AZN 20,000; AZN 200,000 hold	Same thresholds	Same
Record retention	At least 5 years	At least 5 years; documents submitted electronically	Same

New technologies are high risk by default

The AML/CFT Law requires obliged entities to treat relationships and transactions created through new technologies as high risk and to assess risks before launching new products (arts. 8.1, 8.3). The FMS Rules list non-face-to-face use of new technologies, online and mobile services and anonymity-enhancing products as high-risk factors, and non-resident

customers as a high-risk customer type (points 3.9.3, 3.10.2, 3.11.2, 3.11.5). Where new technologies cannot deliver full CDD, the firm must not use them (art. 8.6).

Pending: transfer data rules

Once the CBAR Rule takes effect `Adopted, effective date not yet set`, the originating VASP must hold, verify and pass on the sender's name, identification data and wallet or account, a unique transaction reference, and the beneficiary's name and wallet or account, before the transfer (rules 3.2 to 3.4).

6 Data protection and biometrics

The Law on Personal Data (No 998-IIIQ) applies its full conditions to biometric data, including facial images, fingerprints, iris and retina data and voice samples (art. 9.5). Where consent is the basis, it must be in writing (including through the Electronic Government Information System) and state its validity period and withdrawal conditions (art. 8.2); the controller must prove it (art. 8.4). Collection required by law, such as CDD under the AML/CFT Law, is outside the centralised consent mechanism (art. 8.6), so biometric data used beyond that obligation, for example face recognition at login, needs its own basis such as consent.

Personal data must be destroyed once its purpose is met (art. 9.4), alongside the AML/CFT Law's 5-year minimum retention. Cross-border transfer (art. 14) may proceed regardless of the recipient country's protection level where the data subject consents (art. 14.3). Under Presidential Decree No 361, the Ministry of Digital Development and Transport is the competent authority; since 2 June 2026 its National Cybersecurity Agency (Presidential Decree No 676) keeps the state register of personal data systems and examines complaints (Charter, points 3.1.24, 3.1.25). Failing to protect personal data or to destroy it when required carries a fine of AZN 300 to 500 (Code of Administrative Offences, art. 375.0.2).

7 Sector-specific obligations

Travel Rule and unhosted wallets

Once in force, the CBAR Rule requires the beneficiary VASP to check incoming data and, if incomplete, request it before executing or refuse the transfer, documenting the decision (rules 4.1 to 4.3). Before each transfer the originating VASP must establish whether it goes to another VASP or to an unhosted wallet (one not held by any VASP), assess that risk and

apply limits or prohibitions accordingly (rules 3.6 to 3.8). Data must travel over secure channels that transmit it immediately and in full (rule 5).

Counterparty VASP due diligence

Before dealing with another VASP, a firm must understand its business, check its reputation and supervision, assess its AML controls and obtain senior management approval (rule 6.1). Counterparties in jurisdictions where virtual assets are weakly regulated or unregulated attract enhanced due diligence (rule 6.2).

Sanctions screening

The Law on Targeted Financial Sanctions (No 782-VIQ) covers virtual assets expressly (art. 1.1.5). Every obliged entity must freeze designated persons' assets without delay, meaning immediately or within a few hours (arts. 1.1.11, 3.1.1); UN lists are published automatically on the targeted financial sanctions information resource (art. 5.2).

Tax treatment

Since 2025 the Tax Code classifies virtual assets as intangible assets (art. 13.2.9); it sets no specific identity reporting duty for VASPs.

8 Risk indicators and red flags

Azerbaijan's national risk assessment for 2022 to 2024, summarised in a report published by the FMS, finds that the spread of virtual assets and digital payment platforms has significantly increased the share of cybercrime among predicate offences, that VASPs and virtual-asset-based financial services are a new trend, and that the lack of regulation of virtual assets is a national vulnerability. It also warns that artificial intelligence and deceptive identification and authentication technologies increase manipulation risks for financial institutions.

VIRTUAL ASSET RED FLAGS FROM FMS AND CBAR SOURCES

- **Fake token schemes**: tokens marketed on social media as listed cryptocurrencies, with pyramid-style referral rewards (FMS typology, 2022).
- **Crypto sales disguised as other business**, with company funds run through individuals' cards and accounts (FMS typology, 2022).
- **Regular use of cash and virtual assets** by a business customer (FMS Rules, point 3.9.10).
- **Money mules**: accounts used for other people's purposes (point 3.9.8).
- **Payments from unrelated or unknown third parties** (point 3.13.3).
- **Transfers to or from unhosted wallets** without adequate controls (CBAR Rule 3.7, 3.8).
- **Incomplete originator or beneficiary data** in incoming transfers (CBAR Rule 4.3).
- **Counterparty VASPs** in jurisdictions with weak or no regulation (CBAR Rule 6.2).

9 Enforcement and penalties

Article 598 of the Code of Administrative Offences sets per-breach fines for financial institutions, including VASPs:

Breach	Basis	Officials (AZN)	Legal entities (AZN)
CDD, record-keeping, reliance, PEP or new-technology requirements; internal controls; FMS instructions	Per customer, transaction or instruction, where stated	2,000 to 4,000	20,000 to 30,000
Reporting requirements	Per transaction	2,000 to 4,000	20,000 to 30,000
Failing to hold a transaction as required	Per transaction	3,000 to 5,000	30,000 to 40,000
Ignoring an FMS suspension decision	Per transaction	4,000 to 6,000	40,000 to 50,000

Failing to freeze sanctioned assets	Per person or entity	3,000 to 5,000	30,000 to 50,000

Supervisors must also apply administrative measures and inform the FMS; breaches can lead to suspension or revocation of a licence or registration (AML/CFT Law art. 16.3). The FMS may suspend a transaction for up to 3 working days (art. 15.2). CBAR must also order anyone carrying on licensable financial activity without a licence to stop, publish the finding and refer it to the relevant authority (Law on the Central Bank, art. 51.3).

MONEYVAL's 1st Enhanced Follow-up Report, MONEYVAL(2025)16 (adopted by written procedure on 10 November 2025, published January 2026), kept Azerbaijan "partially compliant" on the virtual asset standard (Recommendation 15) and noted that the FMS guidance on virtual assets remains too generic.

10 Recent changes and what to watch

- **1 January 2027**: new FMS reporting rules `Adopted, effective 1 Jan 2027` (Decision No 3-21-28/3-6-7/2026; start moved from 1 October 2026 by Decision No 3-21-28/3-6-17/2026) add an AZN 50,000 monthly tier for transfers by individuals other than sole proprietors and route reports through the FMS monitoring system.
- **February 2026**: a crypto exchange enters CBAR's regulatory sandbox `Sandbox test, licence exemption`, following four crypto products selected in November 2024; the sandbox is the only official channel for crypto services.
- **November 2025**: MONEYVAL follow-up report `Published January 2026` leaves the virtual asset standard partially compliant; the missing VASP licensing regime remains an open deficiency.
- **April 2025**: Law No 175-VIIQD `In force` requires beneficial owner data on corporate customers to reach the FMS within 3 working days and classifies virtual assets as intangible assets for tax.
- **24 February 2023**: CBAR Rule on virtual asset operations `Adopted, effective date not yet set`. It takes effect once a VASP law is adopted; none exists as of 13 November 2026.

11 What this means for identity verification

- **Documents**: support the Azerbaijani identity card and FİN, and foreign passports and residence permits.

- **Remote method**: build in an strengthened electronic signature (for example ASAN İmza), a database check, two-factor authentication and a live video call or recording.
- **Biometrics**: face recognition can serve as the inherence factor; capture written consent and set deletion rules that respect the 5-year AML minimum.
- **Exclusions**: block remote onboarding of non-resident legal entities and of customers acting through representatives other than a company's legal representative.
- **Interim limits**: cap activity until verification completes, within 5 working days.
- **Re-verification**: refresh CDD yearly for high-risk, every two years for medium and every three for low-risk customers; continuously for PEPs.
- **Transfers**: prepare Travel Rule data capture and unhosted-wallet controls for when the CBAR Rule takes effect.

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 that combines ID document capture, database checks and live video KYC, as required for a first remote relationship.
- Biometric liveness and face match for the inherence factor in strong customer authentication.
- Screening against sanctions, PEP and watchlists at onboarding and on an ongoing basis.
- KYB and beneficial owner verification at the 10% significant-participation threshold.
- No-code workflow builder to block excluded customer types and cap activity until verification completes.

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

- **Cinayət yolu ilə əldə edilmiş əmlakın leqallaşdırılmasına və terrorçuluğun maliyyələşdirilməsinə qarşı mübarizə haqqında Qanun (Law on the Prevention of the Legalization of Criminally Obtained Property and the Financing of Terrorism), No 781-VIQ of 30 December 2022**, consolidated text to 14 July 2026; official English title per fiu.gov.az/en/laws; e-qanun.az, e-qanun.az/framework/53369
- **CBAR Decision No 11/1 of 24 February 2023, Rule for conducting operations with virtual assets in the Republic of Azerbaijan**, e-qanun.az, e-qanun.az/framework/53634
- **Azərbaycan Respublikasının Mərkəzi Bankı haqqında Qanun (Law on the Central Bank), No 802-IIQ**, arts. 50, 51, e-qanun.az, e-qanun.az/framework/5530
- **CBAR Decision No 06/4 of 31 January 2024, Rule on the application of the special regulatory regime**, e-qanun.az, e-qanun.az/framework/56351
- **CBAR, Regulatory sandbox registry**, current and completed projects, sandbox.cbar.az/az/registry and sandbox.cbar.az/az/registry/completed; **CBAR press release, Innovative products identified for testing in Regulatory Sandbox**, 7 November 2024, cbar.az
- **FMS Decision No 3-21-28/3-6-4/2023 of 21 February 2023, Rules on verification measures, identification of risk factors and attribution of the customer profile to risk groups during the application of customer compliance and new technologies**, as amended 14 June 2024, e-qanun.az, e-qanun.az/framework/53641
- **FMS Decision No 3-21-28/3-6-8/2023 of 27 April 2023 on reporting rules and minimum thresholds**, e-qanun.az, e-qanun.az/framework/54120; amended by **FMS Decision No 3-21-28/3-6-7/2026 of 21 April 2026**, and **FMS Decision No 3-21-28/3-6-17/2026 of 25 September 2026**, effective 1 January 2027, both via e-qanun.az/framework/62373
- **Hədəfli maliyyə sanksiyaları haqqında Qanun (Law on Targeted Financial Sanctions), No 782-VIQ of 30 December 2022**, e-qanun.az, e-qanun.az/framework/53362
- **İnzibati Xətalar Məcəlləsi (Code of Administrative Offences)**, arts. 375, 598, e-qanun.az, e-qanun.az/framework/46960
- **Fərdi məlumatlar haqqında Qanun (Law on Personal Data), No 998-IIIQ**, arts. 8, 9, 14, e-qanun.az/framework/19675; **Presidential Decree No 361 of 13 December 2010**, e-qanun.az/framework/21035; **Presidential Decree No 676 of 2 June 2026** and National Cybersecurity Agency Charter, points 3.1.24, 3.1.25, e-qanun.az/framework/61938
- **Elektron imza və elektron sənəd haqqında Qanun (Law on Electronic Signature and Electronic Document), No 602-IIQ of 9 March 2004**, arts. 1, 3, mincom.gov.az; **State Tax Service, ASAN imza (Mobile ID)**, taxes.gov.az
- **Vergi Məcəlləsi (Tax Code)**, art. 13.2.9, e-qanun.az, e-qanun.az/framework/46948
- **FMS, Typology 1 (2022): fake virtual currency trading**, fiu.gov.az

- **FMS, Report on the results of the national risk assessment covering 2022 to 2024**, fiu.gov.az
- **State Tax Service, Taxpayers should obtain an strengthened electronic signature**, 26 April 2024, taxes.gov.az
- **MONEYVAL, Anti-money laundering and counter-terrorist financing measures, Azerbaijan, 1st Enhanced Follow-up Report and Technical Compliance Re-Rating, MONEYVAL(2025)16**, adopted by written procedure on 10 November 2025, Table 1 and R.34, rm.coe.int; published with the **Council of Europe press release "Money laundering and terrorist financing progress reports on Azerbaijan, Croatia and Estonia"**, 23 January 2026, coe.int